CONSERVAÇÃO DE DADOS PESSOAIS NO SETOR DAS COMUNICAÇÕES ELETRÓNICAS E MODALIDADES DE ACESSO PARA EFEITOS DE INVESTIGAÇÃO CRIMINAL (A PROPÓSITO DO ACÓRDÃO *MINISTERIO FISCAL* DO TJUE)

Alessandra Silveira[1]
Pedro Miguel Freitas[2]

O TJUE tem sido confrontado com questões prejudiciais relacionadas com a conservação de dados pessoais por fornecedores de serviços de comunicações eletrónicas. Depois da saga *Digital Rights*[3] e *Tele2,*[4] a trilogia jurisprudencial indispensável neste domínio é agora integrada pelo acórdão *Ministerio Fiscal*[5] de outubro de 2018.[6] O pedido prejudicial foi apresentado no âmbito de um recurso interposto pelo Ministerio Fiscal (Ministério Público espanhol) da decisão do Juzgado de Instrucción n.º 3 de Tarragona (Tribunal de Instrução n.º 3 de Tarragona, a seguir juiz de instrução) sobre a recusa em autorizar o acesso da Polícia Judiciária a dados pessoais conservados pelos fornecedores de serviços de comunicações eletrónicas – e tem por objeto a interpretação de disposições da Diretiva 2002/58 (relativa à privacidade e às comunicações eletrónicas) à luz dos artigos 7.º (proteção da privacidade) e 8.º (proteção de dados pessoais) da Carta dos Direitos Fundamentais da União Europeia (CDFUE).

Com as suas duas questões prejudiciais o órgão jurisdicional nacional pergunta ao TJUE, em substância, se as disposições da Diretiva 2002/58 devem ser interpretadas no sentido de que o acesso de autoridades públicas a dados pessoais, com vista à identificação de titulares de cartões SIM ativados num telemóvel roubado – tais como o apelido, o nome próprio e o endereço –, constitui uma ingerência nos direitos

1 Professora da Escola de Direito e Investigadora CEDU-JusGov, Universidade do Minho. Titular da Cátedra Jean Monnet em Direito da União Europeia (EACEA, Comissão Europeia, Bruxelas).

2 Professor da Universidade Católica Portuguesa (UCP-Porto). Investigador CEDU-JusGov, Universidade do Minho.

3 Acórdão *Digital Rights Ireland*, de 8 de abril de 2014, processos apensos C-293/12 e C-594/12.

4 Acórdão *Tele2*, de 21 de dezembro de 2016, processos apensos C-203/15 e C-698/15.

5 Acórdão *Ministerio Fiscal*, de 2 de outubro de 2018, processo C-207/16.

6 Para acompanhar a saga *Digital Rights* e *Tele2* cfr. Alessandra Silveira e Pedro Freitas, Implicações da declaração de invalidade da Diretiva 2006/24 na conservação de dados pessoais ("metadados") nos Estados-Membros da UE: uma leitura jusfundamental, in *Revista de Direito, Estado e Telecomunicações*, Universidade de Brasília (UnB), vol. 9, n.º 1, 2017, (http://www.ndsr.org/SEER/index.php?journal=rdet); The recent jurisprudence of the CJEU on personal data retention: implications for criminal investigation in Portugal, in UNIO - *EU Law Journal*, vol. 3, No. 2, July 2017 (https://revistas.uminho.pt/index.php/unio/issue/view/24).

fundamentais dos titulares dos dados consagrados na CDFUE *com tal gravidade que esse acesso deva ser limitado (no que tange à prevenção, de investigação, de deteção e de repressão de infrações penais) à luta contra a criminalidade grave*. Em caso afirmativo, *com base em que critérios* se deve apreciar a gravidade da infração em causa?

Assim, como sustenta o Advogado-Geral no considerando n.º 38 das suas Conclusões,[7] o pedido prejudicial tem por objeto a questão de saber se e em que medida o objetivo prosseguido pela regulamentação em causa no processo principal é suscetível de justificar o acesso das autoridades públicas, como a Polícia Judiciária, aos dados pessoais em causa. Ou seja, as questões prejudiciais incidem não sobre as condições da conservação de dados pessoais no setor das comunicações eletrónicas, mas sim sobre as modalidades de acesso das autoridades nacionais a esses dados conservados pelos fornecedores de serviços.

A Diretiva 2002/58 é aplicável ao tratamento de dados pessoais no contexto do fornecimento de serviços de comunicações eletrónicas acessíveis ao público em redes de comunicações públicas na União, incluindo as redes públicas de comunicações que servem de suporte a dispositivos de recolha de dados e de identificação – ou seja, a referida diretiva regula as atividades dos fornecedores de serviços de comunicações eletrónicas. O TJUE tem entendido que as disposições da Diretiva 2002/58 devem ser interpretadas no sentido de que *i*) não só uma medida legislativa que impõe aos fornecedores de serviços de comunicações eletrónicas a conservação dos dados de tráfego e dos dados de localização, *ii*) mas também uma medida legislativa que tem por objeto o acesso das autoridades nacionais aos dados conservados por esses fornecedores *estão abrangidas pelo âmbito de aplicação da diretiva.*

Assim, medidas legislativas que impõem aos fornecedores de serviços de comunicações eletrónicas a conservação de dados pessoais, bem como a obrigação de conceder às autoridades nacionais competentes o acesso a esses dados, implicam necessariamente o tratamento dos referidos dados por parte dos fornecedores de serviços de comunicações. Por conseguinte, tais medidas, dado que regulam as atividades dos referidos fornecedores, não podem ser equiparadas às atividades próprias dos Estados, referidas no artigo 1.º, n.º 3, da Diretiva 2002/58 – que exclui do seu âmbito de aplicação as "atividades do Estado" nos domínios que refere, de entre as quais as atividades no domínio penal e as relacionadas com a segurança pública, a defesa, a segurança do Estado.

Isto releva porque, como veremos em detalhe de seguida, o que está em causa no processo principal que deu origem ao acórdão *Ministerio Fiscal* é o indeferimento de um pedido através do qual a Polícia Judiciária solicita uma autorização judicial

7 Considerando 38 das Conclusões do Advogado-Geral Henrik Saugmandsgaard Øe apresentadas a 3 de maio de 2018 no processo C-207/16.

para aceder a dados pessoais conservados pelos fornecedores de serviços de comunicações eletrónicas – e o TJUE começa por esclarecer que o facto de o referido pedido ter sido apresentado no âmbito de um processo de instrução penal não torna a Diretiva 2002/58 inaplicável ao processo principal. Como salientou o Advogado-Geral no n.º 54 das suas Conclusões,[8] a Diretiva 2002/58 regula qualquer tratamento de dados pessoais no âmbito do fornecimento de serviços de comunicações eletrónicas. Segundo o Advogado-Geral, o conceito de comunicação, na aceção da diretiva, deve ser entendido de uma forma lata, estando o princípio da confidencialidade das comunicações em causa no processo em apreço.

Ademais, em conformidade com o artigo 2.º, segundo parágrafo, alínea b) da diretiva, o conceito de dados de tráfego abrange "quaisquer dados tratados para efeitos do envio de uma comunicação através de uma rede de comunicações eletrónicas ou para efeitos da faturação da mesma". Resulta do considerando 15 da Diretiva 2002/58 que os dados de tráfego podem, nomeadamente, incluir o nome e o endereço do remetente de uma comunicação. Acresce que os dados relativos à identidade civil dos titulares de cartões SIM podem ser necessários para a faturação dos serviços de comunicações eletrónicas fornecidos e integram os dados de tráfego, conforme definidos no artigo 2.º, segundo parágrafo, alínea b), da diretiva. Consequentemente, esses dados estão abrangidos pelo âmbito de aplicação da Diretiva 2002/58.

Fica então claro que, quando se queira saber se se aplicam as garantias da Diretiva 2002/58, não faz mais sentido a tradicional distinção que largo sector da doutrina e jurisprudência portuguesa ainda mantém entre dados de tráfego e de base.[9] Aliás, é a própria distinção tripartida entre dados de tráfego, de base e de conteúdo que fica em causa. Embora se compreenda a razão pela qual tal distinção terá feito sentido, a verdade é que com a Diretiva 2002/58, um ato jurídico europeu com cerca de 17 anos (note-se!), não há qualquer diferença de tratamento jurídico entre os elementos funcionais de uma comunicação (dados de tráfego) e os elementos instrumentais e prévios à comunicação (dados de base ou dados de conexão à rede). Como dissemos acima, é o próprio artigo 2.º, segundo parágrafo, alínea b), da diretiva que faz confluir ambos os tipos de dados a um conceito e regime só, o de dados de tráfego.[10]

---

8 Considerando 54 das Conclusões do Advogado-Geral Henrik Saugmandsgaard Øe apresentadas a 3 de maio de 2018 no processo C-207/16.

9 Cfr. Acórdãos n.º 486/2009 e 420/2017 do Tribunal Constitucional; cfr. Armando Veiga e Benjamim Silva Rodrigues, "A monitorização de dados pessoais de tráfego nas comunicações electrónicas", in *Raízes Jurídicas*, v. 3, n.º 2, jul/dez 2007, pp. 59-110. Em sentido contrário, Acórdão do TRE de 27-01-2011, processo n.º 1276/09.3TAPTM-B.E1.

10 É de notar que a lei portuguesa que transpôs a diretiva – Lei n.º 41/2004, de 18 de agosto – também acata, naturalmente, esta visão, sobretudo no artigo 2.º, n.º 1, al. d), onde se lê que são dados de tráfego "quaisquer dados tratados para efeitos do envio de uma comunicação através de uma rede de comunicações eletrónicas ou para efeitos da faturação da mesma", mas também no artigo 6.º, n.º 2, al. a), em que fica explícito que o tratamento de dados de tráfego necessários

Acompanhando as conclusões do Advogado-Geral Henrik Saugmandsgaard Øe, embora os dados de identificação de um titular de um cartão SIM, ou seja, dados base, não incidam "sobre o «tráfego» de comunicações propriamente dito, na medida em que se afigura que estes dados poderão ser obtidos apesar de ser possível que nenhuma chamada tenha sido feita a partir do aparelho roubado, e, portanto, mesmo que nenhuma comunicação interpessoal tenha sido encaminhada por um operador de telefonia móvel durante o período visado", dever-se-á aplicar a Diretiva 2002/58, "uma vez que o tratamento das informações associadas aos cartões SIM e aos respetivos titulares, objeto do caso vertente, é necessário, de um ponto de vista comercial, à prestação de serviços de comunicações eletrónicas, pelo menos para efeitos de faturação do serviço que é prestado independentemente das chamadas efetuadas ou não no quadro desta prestação"[11].

Indo um pouco mais além, quer a jurisprudência europeia e nacional quer a legislação relevante nesta matéria vai no sentido de que os dados de tráfego e de conteúdo merecem o mesmo tratamento jurídico e proteção contra ingerências indevidas. Por exemplo, o artigo 5.º, n.º 1 da diretiva obriga os Estados-Membros a garantir a tutela da confidencialidade das *comunicações* e *respetivos dados de tráfego*, proibindo 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[12]. Também a nova proposta de Regulamento do Parlamento Europeu e do Conselho relativo ao respeito pela vida privada e à proteção dos dados pessoais nas comunicações eletrónicas mantém o mesmo entendimento no artigo 5.º. No considerando 2 da proposta de Regulamento explica-se o porquê desta equiparação:

> O conteúdo das comunicações eletrónicas pode revelar informações altamente sensíveis acerca das pessoas singulares envolvidas na comunicação, desde experiências e emoções pessoais a condições de saúde, preferências sexuais e opiniões políticas, cuja divulgação poderia resultar em danos pessoais e sociais, prejuízos económicos ou constrangimento. De igual modo, os metadados derivados de comunicações eletrónicas podem também revelar informações muito sensíveis e pessoais. Estes metadados incluem os números ligados, os sítios *web* visitados, a localização geográfica, a hora, a data e duração

à faturação dos assinantes e ao pagamento de interligações abarca o número ou identificação, endereço e tipo de posto do assinante, ou seja, elementos tradicionalmente enquadrados como dados de base. Em face disto, é com alguma perplexidade que assistimos à prolação de acórdãos por tribunais superiores como o Tribunal Constitucional português em que se mantém uma visão ultrapassada sobre o regime jurídico que ser reconhecido aos elementos que tradicionalmente são reconduzidos a dados de base, de tráfego e de conteúdo.

11 Considerandos 52 e 53 das Conclusões do Advogado-Geral Henrik Saugmandsgaard Øe apresentadas a 3 de maio de 2018 no processo C-207/16.

12 Cfr. também o artigo 4.º da Lei n.º 41/2004, de 18 de agosto.

> da chamada, etc., permitindo tirar conclusões precisas relativas à vida privada das pessoas envolvidas na comunicação eletrónica, tais como as suas relações sociais, os seus hábitos e atividades da vida quotidiana, os seus interesses, gostos, etc.

Igualmente relevante é o considerando 14:

> Os dados de comunicações eletrónicas devem ser definidos de uma forma suficientemente abrangente e tecnologicamente neutra de modo a incluírem todas as informações relativas ao conteúdo transmitido ou trocado (conteúdo das comunicações eletrónicas) e as informações relativas a um utilizador final de serviços de comunicações eletrónicas tratadas para efeitos de transmissão, distribuição ou intercâmbio desse conteúdo, incluindo dados que permitam encontrar e identificar a fonte e o destino de uma comunicação, a localização geográfica e a data, hora, duração e o tipo de comunicação. (...) Os metadados de comunicações eletrónicas podem incluir informações que façam parte da subscrição do serviço se essas informações forem tratadas para efeitos de transmissão, distribuição ou intercâmbio de conteúdo de comunicações eletrónicas.

Mesmo a nova proposta de Regulamento do Parlamento Europeu e do Conselho relativo às ordens europeias de entrega ou de conservação de provas eletrónicas em matéria penal, no seu artigo 4.º, n.º 2, confere o mesmo grau de proteção a dados transacionais e a dados de conteúdo, estabelecendo que a ordem europeia de entrega de dados transacionais ou de dados de conteúdo envolverá sempre uma autoridade judicial e só pode ser emitida no caso de infrações penais puníveis no Estado de emissão com uma pena privativa de liberdade de duração máxima não inferior a três anos, ou de infrações específicas possibilitadas por sistemas de informação, ou infrações relacionadas com o terrorismo.

Repare-se que nada obsta à manutenção desta distinção conceptual entre dados de tráfego, dados de base e dados de conteúdo, desde que fique claro que tal distinção não significa necessariamente uma diferença de tratamento jurídico. Por vezes essa diferença de tratamento poderá existir, como parece decorrer da proposta de Regulamento do Parlamento Europeu e do Conselho relativo às ordens europeias de entrega ou de conservação de provas eletrónicas em matéria penal, em que há maior flexibilização das regras em relação à entrega de dados de assinantes ou de dados de acesso, do que acontece quanto a dados transacionais ou de dados de conteúdo. Porém, é a própria proposta de Regulamento que reconhece que apesar de contemplar condições diferentes quanto aos dados de assinantes, por um lado, e quanto aos dados transacionais e de conteúdo, por outro, uma vez que serão diferentes os níveis de interferência nos direitos fundamentais, todas as categorias de dados, sejam dados de assinantes, dados de acesso, dados transacionais e

dados de conteúdo armazenados "contêm dados pessoais, sendo, por conseguinte, abrangidas pelas salvaguardas previstas no acervo da UE em matéria de proteção de dados".

Outras vezes, porém, como vimos, quer os dados de base são colocados num mesmo patamar de importância que os dados de tráfego quer estes últimos são equiparados aos dados de conteúdo.

Voltando então ao caso em análise, atentemos, pois, aos contornos do litígio no processo principal que deu origem ao acordão *Ministerio Fiscal*. Hernandez Sierra foi vítima de roubo no dia 16 de fevereiro de 2015, tendo ficado sem a carteira e um telemóvel. Depois de apresentada queixa nas autoridades policiais, a Polícia Judiciária requereu ao juiz de instrução que ordenasse aos fornecedores de serviços de comunicações eletrónicas o envio dos números de telemóvel ativados no telemóvel roubado, no período de tempo imediatamente posterior ao roubo, mais concretamente entre 16 de fevereiro e 27 de fevereiro de 2015. Para além destes dados, solicitaram ainda a identificação e endereço das pessoas titulares desses números de telefone.

O juiz de instrução indeferiu porém o requerimento com o fundamento de que a medida requerida não seria útil para a identificação do autor do roubo, para além de que a legislação espanhola no domínio da conservação de dados pelos fornecedores de serviços de comunicações eletrónicas (Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones[13]) limitava a transmissão de dados aos casos de infrações graves, conceito que densificado pelo Código Penal espanhol como correspondendo a crimes puníveis com pena de prisão superior a 5 anos. Uma vez que os factos no caso não eram enquadráveis num tipo legal de crime punido com pena de prisão superior a 5 anos, não seria possível, no entender do juiz de instrução, obrigar os fornecedores de serviços de comunicações eletrónicas a transmitir os dados em questão.

Por não concordar com o despacho do juiz de instrução, o Ministério Público espanhol interpôs recurso para a Audiencia Provincial de Tarragona, alegando, *inter alia*, que o roubo constituía uma infração suficientemente grave para justificar a transmissão dos dados por parte dos fornecedores de serviços de comunicações eletrónicas.

Na verdade, a Audiencia Provincial de Tarragona notou que não apenas o Código Penal seria revelante para aferir a gravidade da infração para efeitos da Lei n.º 25/2007, de 18 de outubro. Com a entrada em vigor da Lei Orgânica n.º 13/2015,

13 Lei que transpôs para o ordenamento jurídico espanhol 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, entretanto considerada inválida pelo TJUE no acórdão *Digital Rights*.

de 5 de outubro, operou-se uma importante reforma do Código de Processo Penal relativamente ao fortalecimento das garantias processuais e regulação das medidas de investigação tecnológica. De entre as modificações normativas no Código de Processo Penal merece especial destaque a nova redação do artigo 579.º e a inclusão do artigo 588-B, alínea j), que acabam por influir na própria noção de infração grave. Desde logo o artigo 579.º, n.º 1, do Código de Processo Penal prevê a possibilidade de o juiz de instrução autorizar a interceção da correspondência privada, postal e telegráfica, incluindo fax, burofax e de vales postais internacionais quando o inquérito tenha por objeto crimes dolosos puníveis com uma pena máxima de prisão não inferior a três anos, ou crimes cometidos no âmbito de um grupo ou organização criminosa, ou ainda crimes terroristas.

Assim, passa a haver um critério material de determinação da gravidade de uma infração que assenta na natureza do comportamento criminoso, isto é, se o comportamento puder ser qualificado como um crime cometido no âmbito de um grupo ou organização criminosa ou um crime terrorista terá uma gravidade especialmente intensa atendendo aos bens jurídicos tutelados pelas normas jurídico-penais em causa. Porém, ao lado deste critério material, aparece um outro de natureza formal, alicerçado não na natureza do comportamento e bem jurídico protegido, mas antes no *quantum* punitivo. Por outras palavras, uma infração será grave se for punida de forma igualmente grave, o que, de acordo com o artigo 579.º, se traduz numa punição com pena de prisão superior a três anos.

Chegando a esta conclusão, a Audiencia Provincial de Tarragona questionou, e bem, se crimes punidos com pena de prisão superior a três anos atingem um limiar de gravidade que justifique uma ingerência em direitos fundamentais consagrados na CDFUE. É preciso não esquecer que a grande maioria dos crimes previstos no Código Penal são punidos com pena de pena de prisão superior a três anos e, nessa medida, serão aparentemente graves o suficiente para se permitir o uso de medidas de investigação que implicam uma especial compressão de direitos fundamentais.

É neste enquadramento que a Audiencia Provincial de Tarragona suspende a instância e coloca as seguintes questões prejudiciais:

1 – "Pode a suficiente gravidade dos crimes, enquanto critério que justifica a ingerência nos direitos fundamentais consagrados nos artigos 7.º e 8.º da Carta, ser determinada tendo em consideração unicamente a pena suscetível de ser aplicada ao crime investigado ou, além disso, é necessário identificar na conduta infratora especiais níveis de lesão de bens jurídicos individuais e/ou coletivos?"

2 – "No caso de ser conforme aos princípios constitucionais da União, aplicados pelo TJUE no seu Acórdão de 8 de abril de 2014 [processos apensos C-293/12, *Digital Rights Ireland* e C-594/12, *Seitlinger e o*., EU:C:2014:238] como critérios de fiscalização estrita da Diretiva 2002/58, a determinação da gravidade do crime

atendendo apenas à pena suscetível de ser aplicada, qual deve ser o limiar mínimo desta? Seria compatível com uma norma geral que estabeleça como limite os três anos de prisão?"

Assim, o órgão jurisdicional do reenvio interroga o TJUE sobre os elementos a ter em conta a fim de aferir se as infrações em relação às quais as autoridades policiais podem ser autorizadas a aceder a dados pessoais conservados pelos fornecedores de serviços de comunicações eletrónicas são de gravidade suficiente a justificar a ingerência que tal acesso implica nos direitos fundamentais garantidos nos artigos 7.º e 8.º da CDFUE – conforme interpretados pelo TJUE nos seus acórdãos *Digital Rights* e *Tele2*.

A questão é particularmente relevante porque nesses acórdãos o TJUE declarou que, em matéria de prevenção, de investigação, de deteção e de repressão de infrações penais, apenas a luta contra a criminalidade grave é suscetível de justificar um acesso das autoridades públicas a dados pessoais conservados pelos fornecedores de serviços de comunicações que, considerados no seu conjunto, permitem tirar conclusões precisas sobre a vida privada das pessoas cujos dados estão em causa.

No entanto – é o que resulta esclarecido no acórdão *Ministerio Fiscal* –, o TJUE chama à consideração a gravidade da ingerência nos direitos fundamentais que esse acesso gera. Com efeito, em conformidade com o princípio da proporcionalidade, uma ingerência grave só pode ser justificada, em matéria de prevenção, de investigação, de deteção e de repressão de infrações penais, por um objetivo de luta contra a criminalidade, devendo também esta ser qualificada de grave. Em contrapartida, quando a ingerência que esse acesso implica não for grave, o referido acesso é suscetível de ser justificado por um objetivo de prevenção, de investigação, de deteção e de repressão de infrações penais em geral.[14] Por conseguinte, importava ao TJUE determinar se, no processo em apreço, e em função das circunstâncias do caso concreto, a ingerência nos direitos fundamentais que o acesso da Polícia Judiciária aos dados em causa implica deve ser considerada como sendo grave.

O TJUE considerou que o pedido em causa no processo principal, através do qual a Polícia Judiciária solicitava, para efeitos de uma investigação penal, a autorização judicial para aceder a dados pessoais conservados pelos fornecedores de serviços de comunicações eletrónicas, tinha por único objetivo identificar os titulares dos cartões SIM ativados durante um período de 12 dias com o código do telemóvel roubado. O pedido visava apenas o acesso aos números de telefone correspondentes a esses cartões SIM e aos dados relativos à identidade civil dos titulares dos referidos cartões, tais como o apelido, o nome próprio e, sendo caso disso, o endereço. No entanto, esses dados não tinham por objeto, como confirmaram o Governo espanhol e o Ministério Público na audiência, as comunicações efetuadas com o telemóvel

14 Acórdão *Ministerio Fiscal*, de 2 de outubro de 2018, processo C-207/16, considerandos 55 a 57.

roubado nem a sua localização.

Desta forma, os dados visados pelo pedido de acesso em causa no processo principal permitiam apenas associar, durante um determinado período, o cartão ou os cartões SIM ativados no telemóvel roubado à identidade civil dos titulares desses cartões SIM. Sem um cruzamento com os dados relativos às comunicações efetuadas com os referidos cartões SIM e os dados de localização, esses dados não permitem conhecer a data, a hora, a duração e os destinatários das comunicações efetuadas com o ou os cartões SIM em causa, nem os locais onde essas comunicações tiveram lugar ou a frequência destas com determinadas pessoas durante um dado período. Ou seja, os referidos dados não permitiam tirar conclusões precisas a respeito da vida privada das pessoas cujos dados estavam em causa. Nessas condições, entendeu o TJUE que o acesso aos dados não podia ser qualificado como uma ingerência grave nos direitos fundamentais dos titulares.[15]

Assim, o TJUE concluiu que a ingerência que implica o acesso aos dados em causa é suscetível de ser justificada pelo objetivo de prevenção, de investigação, de deteção e de repressão de infrações penais em geral, ao qual se refere o artigo 15.º, n.º 1, primeira frase, da Diretiva 2002/58, sem que seja necessário que tais infrações sejam qualificadas de graves. Ou nos exatos termos da decisão do TJUE: "o acesso das autoridades públicas aos dados com vista à identificação dos titulares dos cartões SIM ativados num telemóvel roubado, tais como o apelido, o nome próprio e, sendo caso disso, o endereço desses titulares, constitui uma ingerência nos direitos fundamentais destes últimos, consagrados nesses artigos da Carta, que não apresenta uma gravidade tal que esse acesso deva ser limitado, em matéria de prevenção, de investigação, de deteção e de repressão de infrações penais, à luta contra a criminalidade grave."[16]

À guisa de conclusão, diríamos que da trilogia *Digital Rights, Tele2, Ministerio Fiscal* deriva que (e aqui acompanhamos a sageza de José Luís da Cruz Vilaça a propósito do tema): *i*) há que proceder, em cada caso, a uma criteriosa avaliação da situação tendo em conta, por um lado, a gravidade da ingerência nos direitos fundamentais e, por outro, a gravidade da infração sob investigação; *ii*) o escrutínio do TJUE tende a ser mais intenso quando se trate de traçar um equilíbrio adequado entre direitos e liberdades individuais, por um lado, e imperativos de ordem e de segurança públicas, por outro, tanto mais que estes são suscetíveis de envolver igualmente a preservação de direitos de caráter tão fundamental como o direito à vida e à integridade física.[17]

15 Acórdão *Ministerio Fiscal*, de 2 de outubro de 2018, processo C-207/16, considerandos 59 a 61.

16 Acórdão *Ministerio Fiscal*, de 2 de outubro de 2018, processo C-207/16, considerando 63.

17 Cfr. José Luís da Cruz Vilaça, The digital world and the new frontiers of the European courts case-law, in UNIO – *EU Law Journal*, vol. V, No.1, 2019, p. 14-15 (https://revistas.uminho.pt/index.php/unio/).