De LEGIBUS

3

Julho de 2022

A LEI DOS "METADADOS": A CRÓNICA DE UMA MORTE HÁ MUITO ANUNCIADA

José Grazina Machado

Revista de Direito

Law Journal

Faculdade de Direito — Universidade Lusófona

https://revistas.ulusofona.pt/index.php/delegibus

A LEI DOS "METADADOS": A CRÓNICA DE UMA MORTE HÁ MUITO ANUNCIADA*

José Grazina Machado**

Sumário: 1. Enquadramento; 2. O conceito de dado pessoal e o equívoco do "metadado"; 3. A Diretiva 2006/24/CE; 4. A Lei n.º 32/2008; 5. O acórdão de 8 de abril de 2014 do Tribunal de Justiça da União Europeia; 6. O acórdão de 21 de dezembro de 2016 do Tribunal de Justiça da União Europeia; 7. O acórdão n.º 268/2022 do Tribunal Constitucional. 8. Conclusões sumárias.

Resumo: A um tempo, o presente artigo visa clarificar o conceito de dados pessoais, desfazendo os equívocos inerentes à utilização de um conceito não empregue no Direito da Proteção de Dados Pessoais, como é: o metadado.

A outro tempo desenvolve-se uma breve resenha, numa perspetiva evolutiva, sobre a comummente denominada Lei dos "Metadados", procurando demonstrar que as recentes questões de inconstitucionalidade apreciadas e decididas pelo Tribunal Constitucional não se afiguram inovadoras no ordenamento jurídico.

Por fim, formularemos nas conclusões sumárias, uma apreciação global da temática, deixando algumas pistas para assegurar a compatibilidade material do diploma nacional com a Constituição da República Portuguesa.

Palavras-Chave: A Lei dos Metadados; Direito da Proteção de Dados Pessoais; Dado Pessoal

Abstract: At one time, this article aims to clarify the concept of personal data, undoing the mistakes inherent in the use of a concept not used in the Law of Protection of Personal Data, such as: metadata.

At another time, a brief review is developed, from an evolutionary perspective, on the commonly called "Metadata" Law, seeking to demonstrate that the recent

* O presente artigo foi submetido no dia 29 de maio de 2022, ainda antes de ter sido apresentada na Assembleia da República a Proposta de Lei n.º 11/XV/1.ª do Governo que "regula o acesso a metadados referentes a comunicações eletrónicas para fins de investigação criminal", bem como os diversos Projetos de Lei apresentados pelos partidos políticos.

** Professor Assistente da Faculdade de Direito da Universidade Lusófona (Lisboa) e doutorando em Direito na Faculdade de Direito da Universidade Lusófona (Lisboa). Investigador Convidado no Centro de Estudos Avançados em Direito Francisco Suárez (CEAD). O autor exerce, atualmente, as funções de Vogal da Comissão Nacional de Proteção de Dados, mas o presente artigo reflete apenas a sua perspetiva, pelo que nada do que aqui é afirmado pode ser imputado a esta entidade pública.

issues of unconstitutionality considered and decided by the Constitutional Court do not appear to be innovative in the legal system.

Finally, we will formulate in the summary conclusions, a global appreciation of the theme, leaving some clues to ensure the purpose pursued by the national law with the Constitution of the Portuguese Republic.

Keywords: The Metadata Law; Right of Protection of Personal Data; Personal Data

1. Enquadramento

O presente artigo tem por objeto explicitar os principais marcos jurisprudenciais europeus e nacional que culminaram com o recente acórdão proferido pelo Tribunal Constitucional (doravante, TC), n.º 268/2022, proferido no processo n.º 828/2019, na sequência de um processo de fiscalização abstrata sucessiva[1] da constitucionalidade, por um lado.

Por outro, no hodierno artigo analisa-se o conceito de dados pessoais, desfazendo os equívocos inerentes à utilização de um conceito não empregue no Direito da Proteção de Dados Pessoais, como é: o metadado.

Esta delimitação positiva do objeto exclui algumas matérias ou assuntos que próximos do tema, não serão aflorados. É o caso do acórdão n.º 382/2022, do Tribunal Constitucional (doravante, TC).

Ora, em agosto de 2019, a Provedora de Justiça requereu a apreciação e declaração, com força obrigatória geral, da inconstitucionalidade das normas constantes dos artigos 4.º, 6.º e 9.º da Lei n.º 32/2008, de 17 de julho (doravante, Lei n.º 32/2008).

Tal diploma regula a conservação e transmissão dos dados de tráfego e de localização relativos a pessoas singulares e coletivas, bem como os dados conexos, referente à identificação do assinante ou do utilizador registado, para fins de investigação, deteção e repressão de crimes graves por parte das autoridades competentes.

Com efeito, o ato normativo transpôs para a ordem jurídica interna a Diretiva 2006/24/CE, do Parlamento e do Conselho, de 15 de março (doravante, Diretiva 2006/24/CE).

Ante diversas notícias veiculadas pelos órgãos de comunicação social nacionais, além de várias posições expressas por comentadores, justifica-se clarificar dogmaticamente o conceito de dado pessoal, com o propósito de aquilatar se, de facto, e de direito, o conceito de "metadado" existe, a um tempo.

1 Está em causa, "O controlo abstrato sucessivo, também chamado de controlo em 'via principal'; em via de 'ação', ou em 'via direta' (cf. art. 281.º), existe quando, independentemente de um caso concreto, se averigua da conformidade de quaisquer normas com o parâmetro normativo-constitucional. O Tribunal Constitucional atua como 'defensor da Constituição' relativamente ao legislador e como órgão de garantia da 'legalidade reforçada'", José Joaquim Gomes Canotilho, *Direito Constitucional e Teoria da Constituição*, 7.ª edição, (Coimbra: Almedina, 2003), 1005.

A outro tempo, importa perscrutar a jurisprudência europeia, que há já largos anos se pronunciara pela invalidade da Diretiva, facto aparentemente desconhecido por alguns setores da comunidade jurídica nacional.

Ainda noutro plano justificar-se-á, até pelas consequências fácticas e jurídicas emergentes do aresto proferido pelo TC, sugerir algumas pistas que permitam compatibilizar de *lege ferenda*, uma solução normativa com a Constituição da República Portuguesa (doravante, CRP). Sobretudo ante o conflito de bens jurídicos e de direitos fundamentais, particularmente do direito à segurança, com o direito à reserva da vida privada, com a inviolabilidade das comunicações, o direito à proteção dos dados pessoais, bem como o princípio da proporcionalidade.

No que diz respeito à importância do tema, assinala-se que se reveste de elevada pertinência dogmática (teórica e prática), mercê da decisão proferida pelo TC resultar uma multiplicidade de consequências jurídicas com profundos impactos, *maxime* de natureza pessoal. Por exemplo, os titulares dos dados, particularmente aqueles que tenham sido condenados em processo-crime e as informações (dados de tráfego e de localização) tenham servido de prova dos factos integradores do tipo legal de crime imputado, poderão suscitar a reabertura de tais processos; os fornecedores de serviços de comunicações eletrónicas, que atuam na qualidade de responsáveis pelos tratamentos de dados pessoais, as autoridades policiais e serviços de segurança que acederam a tal informação e terão de proceder ao apagamento dos dados pessoais em causa, ou então as próprias autoridades judiciárias, além das autoridades policiais que terão de reequacionar a utilização dos meios de prova recolhidos, ou a obter, no decurso de processos criminais pendentes, ou futuros. A relevância resulta ainda da clarificação de alguns conceitos empregues que, a nosso ver, se afiguram tecnicamente incompatíveis. A par destes argumentos milita ainda a defesa, não menos pertinente, dos direitos fundamentais à reserva da vida privada e familiar (cf. n.º 1 do art. 26.º da CRP), como também da proteção dos dados pessoais (cf. artigo 35.º da CRP), ante os fins de investigação, deteção e repressão de crimes.

Relativamente à razão de ordem justifica-se abordar primeiramente o conceito de dado pessoal para depois nos debruçarmos sobre o conceito de "metadado". A seguir aflorar-se-ão os impactos que os dados de tráfego e de

localização comportam na vida das pessoas físicas. Depois examinaremos as principais decisões em matéria de jurisprudência europeia e nacional sobre a temática em apreço. Por fim, formularemos as conclusões finais, em que apresentaremos algumas soluções que podem ser adotadas num novo diploma legislativo que, segundo diversas notícias avançadas pelos órgãos de comunicação social nacionais, será emanado a breve trecho. Crê-se que a razão de ordem exposta permite a compreensão da temática em toda a sua extensão, facultando uma visão global e evolutiva ao leitor.

A apreciação efetuada será de cariz puramente dogmático, ainda que a matéria objeto de análise se sujeite a diversas reflexões de cariz filosófico e político.

2. O conceito de dado pessoal e o equívoco do "metadado"

Ao tempo da entrada em vigor da Diretiva 2006/24/CE, encontrava-se em vigor a Diretiva 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, transposta para o ordenamento jurídico nacional, através da Lei n.º 67/98, de 26 de outubro, atualmente revogada pela Lei n.º 58/2019, de 8 de agosto.

Na Diretiva 95/46/CE, o conceito de dado pessoal era definido pela al. *a*) do artigo 2.º, que dispunha:

- "[...] qualquer informação relativa a uma pessoa singular identificada ou identificável ("pessoa em causa"); é considerado identificável todo aquele que possa ser identificado, direta ou indiretamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social".

Este conceito não foi objeto de significativas alterações no âmbito do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 (doravante, RGPD).

Aí o conceito foi densificado na al. *1*) do artigo 4.º nos seguintes termos:

– "[...] informação relativa a uma pessoa singular identificada ou identificável ('titular dos dados'); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de

identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular.".

A este propósito sinaliza-se que:

– "A distinção entre os conceitos de dados de pessoais previstos no RGPD e na Diretiva 95/46/CE consiste(m) em:

a) Enquanto que a Diretiva refere "pessoa em causa", o RGPD menciona o 'titular dos dados pessoais';

b) Ao invés da Diretiva, o RGPD menciona especificamente 'dados de localização' e 'identificadores por via eletrónica';

c) O RGPD menciona em especial dados genéticos, ao contrário da Diretiva;

d) O RGPD menciona, a título de exemplo, dados de caráter mental, substituindo os dados psíquicos da Diretiva."[2]

Com o RGPD é efetuado um recorte concetual de três modalidades de dados, em que o legislador europeu optou por definir um conceito determinado ou preciso quanto aos dados genéticos, dados biométricos e dados relativos à saúde (cf. als. *13*), *14*) e *15*) do art. 4.º). Em sentido inverso, da Diretiva 95/46/CE não constavam as sobreditas modalidades de dados pessoais.

Acresce ainda que a al. *a*) do n.º 2 do artigo 2.º da Diretiva 2006/24/CE apenas delimita por dados:

– "[...] os dados de tráfego e os dados de localização, bem como os dados conexos necessários para identificar o assinante ou o utilizador."

Com estes pressupostos, importa ter presente que de ambos os diplomas não resulta o conceito metadado.

Na doutrina, por cá, no Direito da Proteção de Dados Pessoais, Barreto Menezes Cordeiro elabora uma leitura exegética do conceito de dado pessoal, recortando-o em quatro elementos: "[...] (i) qualquer informação; (ii) relativa a; (iii) pessoa singular; e (iv) identificada e identificável"[3]. O autor

2 Alexandre Sousa Pinheiro, *Comentário ao Regulamento Geral de Proteção de Dados,* (Coimbra, Almedina, 2018), 121.

3 Barreto Menezes Cordeiro, *Direito da Proteção de Dados à luz do RGPD e da Lei n.º 58/2019*, (Coimbra, Almedina, 2020), 107.

acentua a diferenciação entre pessoa identificada ou identificável, a qual já resulta *expressis verbis* da al. *1*) do artigo 4.º do RGPD.

Lá fora, Alberto De Franceschi destaca o conteúdo amplo do conceito, assinalando ainda que a informação pode não coincidir com os dados, mas promana de uma elaboração dos dados[4]. Outrossim, este autor não procede a nenhuma qualificação de supradados/metadados ou infradados.

Na jurisprudência europeia, o acórdão de 8 de abril de 2014, do Tribunal de Justiça da União Europeia (doravante, TJUE), mais conhecido por Tele2, que adiante se aflorará, também não emprega tal conceito, à semelhança do acórdão de 21 de dezembro de 2016, do TJUE, crismado de Digital Rights.

Já na justiça constitucional nacional, no acórdão 420/2017 proferido pelo TC no âmbito de um processo de fiscalização da constitucionalidade concreta, o qual versou sobre a temática cujo aresto adiante abordaremos, aludiu-se ao conceito de metadados. Naquele aresto deixou-se expendido: "O objeto do presente recurso está relacionado com os designados 'metadados', usualmente definidos como 'dados sobre dados', por dizerem respeito a circunstâncias das comunicações e não ao próprio conteúdo da comunicação (Acórdão n.º 403/2015, ponto 9)."[5] Este acórdão, que é referenciado pelo transcrito, refere-se à apreciação da questão de inconstitucionalidade atinente à norma do n.º 2 do artigo 78.º do Decreto n.º 426/XII da Assembleia da República que "Aprova o Regime Jurídico do Sistema de Informações da República Portuguesa", por violação do n.º 4 do artigo 34.º da CRP. Aliás, o conceito "metadados" viria a ser replicado no âmbito do acórdão do TC que abordaremos. Acresce ainda que tal alusão consta ainda do pedido de declaração de inconstitucionalidade formulado pela Provedora de Justiça.

Ora, o conceito "metadados", embora pareça resultar de uma construção jurisprudencial exclusivamente nacional, pode conduzir a leituras dúbias, por inculcar que poderá não se tratar de dados pessoais, por referente a informação não pessoais.

Note-se que no campo dogmático e jurisprudencial apenas se emprega o conceito de dados pessoais, pelo que os dados de tráfego e de localização se

4 Alberto De Franceschi, *Codice Della Privacy e Data Protection*, (Giuffrè Editore, 2021), 158.

5 Disponível em http://www.tribunalconstitucional.pt/tc/acordaos/20170420.html (consultado em 23.05.2022).

reconduzem àquela categoria, por corresponderem a informação relativa a uma pessoa singular, identificada ou identificável (embora esmagadoramente a identificada). Tecnicamente, o conceito de dados pessoais, com o halo concetual acima aflorado no quadro da Diretiva 2006/24/CE, contempla os dados de tráfego e de localização, irrelevando se se afiguram sequenciais ou não. Por exemplo, o titular dos dados que realize análises clínicas, ao facultar os dados de identificação e de faturação e posteriormente as amostras biológicas para o efeito, assim como os resultados bioquímicos gerados, não transformam estes últimos em metadados, por se tratar de dados gerados sobre dados. O que não se confunde com a especial tutela jurídica conferida aos segundos e terceiros, por relativos à saúde do titular dos dados.

Por conseguinte, o conceito de metadados não tem acolhimento normativo europeu ou nacional, nem doutrinal, nem jurisprudencial no plano europeu, resultando de uma construção jurisprudencial nacional, que criou um conceito replicado de forma acrítica e sem tecnicidade.

Numa operação de tratamento de dados pessoais como seja o envio de um SMS[6], um MMS[7], uma chamada telefónica ou uma mensagem de correio eletrónico perfilam-se, em regra, quatro categorias de dados pessoais: dados base (identificação e faturação), dados de tráfego, dados de localização do dispositivo e os dados relativos ao conteúdo da comunicação propriamente dita.

Pelo que o conceito "metadados" não deverá ser relevado, uma vez que estão em causa dados de tráfego e dados de localização. Trata-se de informações relativas a pessoas singulares identificadas, gozando de idêntica proteção legal, não constituindo um conceito autónomo, nem assumindo relevância dogmática diversa, razões que deverão afastar o uso, em sentido técnico-jurídico, de tal conceito, representando a nosso ver, um equívoco.

6 Serviços de mensagens curtas, cf. n.º 1 do artigo 13.º - A da Lei n.º 41/2004, de 18 de agosto, na atual redação.

7 Serviços de mensagem multimédia, cf. n.º 1 do artigo 13.º - A da Lei n.º 41/2004, de 18 de agosto, na atual redação.

3. A Diretiva 2006/24/CE

A história da Lei n.º 32/2008 principia com a Diretiva 2006/24/CE.

A sobredita fonte de Direito derivado da União Europeia (doravante, UE) teve diversos pressupostos. *Prima facie*, os Estados-Membros terem aprovado legislações internas referentes à conservação de dados pelos fornecedores de serviços tendo em vista a prevenção, investigação, deteção e repressão de infrações penais[8], ou até nem disporem de legislação interna a esse propósito. O que conduziu a disparidades legislativas e técnicas entre disposições plasmadas nas respetivas legislações[9]. Essas disparidades residiam, no essencial, na definição das categorias e tipos de dados de tráfego e de localização a conservar, além das condições e prazos de conservação de tais dados[10], por um lado.

Por outro, a Diretiva em apreço reconheceu a relevância de tais dados pessoais para a investigação, deteção e repressão de infrações penais.

Ademais assinala-se que a Diretiva 2006/24/CE apenas teve por objeto os dados pessoais: tráfego e de localização. Excluídos ficaram aqueles que se reportam ao conteúdo das comunicações ou serviço de comunicações.[11]

Por fim, importa ainda ter presente que a fonte de direito em apreço vincula os Estados-Membros destinatários quanto aos resultados a alcançar, relegando para estes, a definição dos meios[12]. Pelo que têm, outrossim, o dever[13] de transpor a Diretiva para o direito interno.

Com este pano de fundo foi adotada a Diretiva que entrou em vigor 20 dias após a publicação no *Jornal Oficial da União Europeia* – 13 de abril de 2006. Note-se que a transposição da Diretiva deveria ocorrer até ao dia 15 de setembro de 2007.[14] Todavia, houve um vasto conjunto de Estados-Membros, em que se não inclui Portugal, os quais aproveitando a cláusula de

8 Cf. considerando 5 da Diretiva.

9 Cf. considerando 6 da Diretiva.

10 Cf. considerando 6 da Diretiva.

11 Cf. considerando 13 da Diretiva.

12 Cf. artigo 288.º, 3.º parágrafo do TFUE.

13 Cf. Ana Guerra Martins, *Manual de Direito da União Europeia*, 2.ª Edição, (Coimbra: Almedina, 2017), 499.

14 Cf. n.º 1 do artigo 15.º da Diretiva.

abertura contida no n.º 3 do artigo 15.º da Diretiva, diferiram temporalmente a transposição do diploma, desde que notificassem o Conselho e a Comissão, por declaração. Foram os casos dos Países Baixos, Áustria, Estónia, Reino Unido, Chipre, Grécia, Luxemburgo, Eslovénia, Suécia, Lituânia, Letónia, República Checa, Bélgica, Polónia, Finlândia e da Alemanha que adotaram prazos não coincidentes.

O diploma instituiu a obrigação de conservação de dados no n.º 1 do artigo 5.º, sob a epígrafe "Categorias de dados a conservar", estabelecendo um elenco, fechado, por típico e taxativo, a reter:

– "Os Estados-Membros devem assegurar a conservação das categorias de dados seguintes em aplicação da presente directiva:

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) marcados (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.".

Sublinha-se que tais dados de tráfego e de localização, cuja obrigação de conservação ali se sedimentou, abrangeu a totalidade das pessoas singulares, como também das pessoas coletivas, além dos dados conexos necessários para identificar o assinante ou o utilizador registado.[15] Este é um dos aspetos de regime que será retomado adiante, no âmbito da jurisprudência europeia firmada a este propósito.

Do elenco de categorias de dados pessoais já se pode extrair que as informações em causa contendem com a vida privada e permitem extrair um conjunto de factos e respetivas inferências de comportamento das pessoas físicas. Para melhor ilação, destacam-se como exemplos os hábitos da vida quotidiana, os lugares onde se encontram de forma permanente ou temporária, as atividades praticadas, a duração destas, os contactos efetuados, a duração e periodicidade de tais interações, o período de permanência na internet, os meios sociais frequentados, entre outros, detendo um profundo impacto na vida privada e familiar dos titulares dos dados.

15 Cf. n.º 2 do artigo 1.º da Diretiva.

A obrigação de conservação impendia exclusivamente sobre as entidades fornecedoras de serviços de comunicações eletrónicas publicamente disponíveis, ou de uma rede pública de comunicações, assumindo aquelas a posição jurídica de responsáveis pelo tratamento de dados pessoais. Este conceito, preciso ou determinado, encontra-se densificado na alínea *7*) do artigo 4.º do RGPD e poderá ser uma pessoa física ou uma pessoa jurídica, de direito privado ou de direito público, aduzindo o RGPD, a autoridade pública, a agência ou outro organismo que determine as finalidades e os meios de tratamento de dados pessoais. Trata-se de um conceito funcional.[16] Com efeito, em causa estava uma operação material de tratamento de dados pessoais: conservação[17], contendendo, portanto, com o direito à proteção dos dados pessoais.

O artigo 6.º da Diretiva 2006/24/CE fixou outra cláusula de abertura, ao estabelecer um hiato tempo, não inferior a seis meses e não superior a dois anos, no máximo, para assegurar a conservação de tais dados. Tal cláusula relegou para os legisladores nacionais, no quadro da transposição, a liberdade legiferante para determinar o prazo a adotar, embora circunscrito aos limites temporais referenciados.

A par da fixação do prazo, a Diretiva 2006/24/CE estabeleceu ainda outra operação de tratamento de dados pessoais, desta feita prevista no artigo 4.º. Aí se afirma que os Estados-Membros deverão assegurar que os dados pessoais serão transmitidos às autoridades nacionais competentes em casos específicos e segundo a legislação nacional. Tal pressupunha a fixação do elenco das autoridades nacionais que poderiam aceder aos dados de tráfego e de localização, assim como os procedimentos e condições de acesso. Assinala-se que da epígrafe do artigo 4.º da Diretiva 2004/24/CE consta o conceito de acesso. Todavia, na verdade, o que está em causa é uma operação de comunicação

16 Cf. Comité Europeu de Proteção de Dados, *Orientações 7/2020 sobre os conceitos de responsável pelo tratamento e subcontratante no RGPD,* versão 2.0, adotadas em 7 de julho de 2021, p. 10, disponíveis em https://edpb.europa.eu/system/files/2022-02/eppb_guidelines_202007_controllerprocessor_final_pt.pdf (consultadas em 21.05.2022).

17 Relativamente a esta operação, "No seu preenchimento mais comum, conservar significa manter em bom estado, evitando que se estrague, altere ou pereça. Mas o sentido com que o termo é empregue poderá não ser este. Na versão inglesa e na versão alemã é utilizada a expressão armazenamento, o que nos remete para uma operação de natureza distinta.", Barreto Menezes Cordeiro, *Direito da Proteção de Dados à luz do RGPD e da Lei n.º 58/2019*, (Coimbra: Almedina, 2020), 146.

de dados pessoais, visto que os fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações transmitiam às autoridades a determinar por cada Estado-Membro o conjunto dos dados de tráfego e de localização conservados. Conquanto, a operação não corresponde tecnicamente a um acesso, mas antes a comunicação de dados pessoais, integrando o conceito de divulgação por transmissão, contido na al. *2*) do artigo 4.º do RGPD. Na verdade, há uma transmissão de um conjunto de dados pessoais de uma pessoa jurídica para outra. O próprio conceito de acesso não consta do amplo catálogo de operações de tratamento referenciadas naquele preceito, sendo apenas empregue no âmbito do exercício do direito de acesso do titular dos dados, previsto no artigo 15.º do RGPD.

4. A Lei n.º 32/2008

Preliminarmente, compulsando o brevíssimo preâmbulo do diploma se infere que não foi solicitada a emissão de parecer a um conjunto de entidades que poderiam ter emitido um juízo qualificado sobre a proposta de diploma, como, por exemplo, a Comissão Nacional de Proteção de Dados (doravante, CNPD), a Ordem dos Advogados, o Conselho Superior do Ministério Público ou o Conselho Superior da Magistratura, entre outras que se poderiam apontar para o efeito.

No âmbito nacional, a Diretiva 2006/24/CE foi transposta através da Lei n.º 32/2008, de 17 de julho. Tal diploma replicou, em larga medida, parte dos preceitos contidos na Diretiva, pelo que se justifica perscrutar as opções tomadas pelo legislador, no âmbito das cláusulas de abertura contidas nas normas da Diretiva e acima explicitadas.

Desde logo, foi definido o conceito de autoridades competentes, compreendendo as autoridades judiciárias e as autoridades de polícia criminal: Polícia Judiciária, Guarda Nacional Republicana, Polícia de Segurança Pública, Polícia Judiciária Militar, Serviço de Estrangeiros e Fronteiras e Polícia Marítima.[18] Note-se que este conceito opera no quadro do presente diploma.

18 Cf. al. *f*) do n.º 1 do artigo 2.º da Lei n.º 32/2008.

De igual modo formou-se o conceito de crime grave, autoexplicativo, aludindo aos "crimes de terrorismo, criminalidade violenta, criminalidade altamente organizada, sequestro, rapto e tomada de reféns, crimes contra a identidade cultural e integridade pessoal, contra a segurança do Estado, falsificação de moeda ou de títulos equiparados a moeda, contrafação de cartões ou outros dispositivos de pagamento, uso de cartões ou outros dispositivos de pagamento contrafeitos, aquisição de cartões ou outros dispositivos de pagamento contrafeitos, atos preparatórios da contrafação e crimes abrangidos por convenção sobre segurança da navegação aérea ou marítima;".[19] Trata-se de um elenco taxativo. Sublinha-se que este conceito não encontra respaldo, *v.g.*, no Código de Processo Penal (doravante, CPP). Esta definição abrange conceitos positivados e densificados naquele diploma processual penal, como terrorismo[20], criminalidade violenta[21], ou criminalidade altamente organizada[22], postergando aparentemente o conceito de criminalidade especialmente violenta, que se encontra desenvolvido naquele diploma adjetivo.

O amplo conjunto de autoridades policiais que podiam solicitar a comunicação dos dados de tráfego e de localização é contraditório no plano sistémico nacional. Desde logo, com a Lei de Organização da Investigação Criminal, dado que a investigação de uma parte significativa dos ilícitos penais que integram tais conceitos corresponde à competência reservada da Polícia Judiciária, não podendo ser sequer deferida em outros órgãos de polícia criminal.[23] O que não deixa de constituir um paradoxo, permitir a transmissão de tais dados a órgãos de polícia criminal que por ser turno não têm competência para investigar parte dos crimes subsumíveis ao conceito de crime grave acima transcrito.

Depois foi determinado o prazo de um ano, a contar da data da conclusão da comunicação, para a obrigação de conservação dos dados de tráfego e de localização (replicados no art. 4.º da Lei), nos termos do artigo 6.º da Lei n.º 32/2008.

19 Cf. al. *g*) do n.º 1 do artigo 2.º da Lei n.º 32/2008.

20 Al. *i*) do artigo 1.º do Código de Processo Penal.

21 Al. *j*) do artigo 1.º do Código de Processo Penal.

22 Al. *m*) do artigo 1.º do Código de Processo Penal.

23 Cf. n.º 2 do artigo 7.º da Lei n.º 49/2008, de 27 de agosto, na atual redação.

No que diz respeito à comunicação dos dados "[...] só pode ser autorizada, por despacho fundamentado do juiz de instrução, se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter no âmbito da investigação, deteção e repressão de crimes graves", à luz do n.º 1 do artigo 9.º, desde que requerida pelo Ministério Público ou pela autoridade de polícia criminal competente, de acordo no n.º 2. No que lhe concerne, o n.º 3 do artigo 9.º da Lei n.º 32/2008 estabeleceu que tal comunicação apenas poderia ser autorizada relativamente a suspeito ou arguido, "[...] que sirva de intermediário, relativamente à qual haja fundadas razões para crer que recebe ou transmite mensagens destinadas ou provenientes de suspeito ou arguido", ou vítima de crime, mediante consentimento efetivo ou presumido, em harmonia com as als. *a*), *b*) e *c*) do n.º 3 do artigo 9.º.

Note-se que o TC já havia apreciado, pelo menos num processo de fiscalização da constitucionalidade concreta, as questões de inconstitucionalidade referentes ao artigo 4.º da Lei n.º 32/2008, mormente no acórdão n.º 420/2017, de 13 de julho de 2017.[24] Neste aresto, o TC decidiu não julgar inconstitucional a norma atinente à obrigação de conservação que impende sobre os fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações.

5. O acórdão de 8 de abril de 2014 do Tribunal de Justiça da União Europeia

Deixando de parte os parâmetros europeus e nacionais definidos pelos respetivos legisladores, é tempo de aquilatar a jurisprudência europeia. Para tanto, opta-se por identificar as partes, as questões prejudiciais, bem como a apreciação jurídica ali tecida e os dispositivos dos dois arestos selecionados.

O primeiro acórdão que versou sobre a Diretiva 2006/24/CE reportou-se à suscitação de pedidos de decisão prejudicial, nos processos apensos C-203/15 e C-698/15, com fundamento no artigo 267.º do Tratado

24 Disponível em http://www.tribunalconstitucional.pt/tc/acordaos/20170420.html (consultado em 22.05.2022).

de Funcionamento da União Europeia. O processo foi apresentado pelo Kammarrätten i Stockholm (Tribunal Administrativo de Segunda Instância de Estocolmo, Suécia) e pela Court of Appeal (England & Wales) (Civil Division) [Tribunal de Segunda Instância (Inglaterra e País de Gales) (Secção Cível), Reino Unido], referente a duas decisões, respetivamente, de 29 de abril de 2015 e de 9 de dezembro de 2015, entradas no Tribunal de Justiça em 4 de maio de 2015 e em 28 de dezembro de 2015, nos processos que opuseram Tele2 Sverige AB contra Post-och telestyrelsen, e ainda Secretary of State for the Home Department (C-698/15) contra Tom Watson, Peter Brice, Geoffrey Lewis.

No primeiro processo foram suscitadas as seguintes questões prejudiciais:

– "1) É compatível com o artigo 15.º, n.º 1, da Diretiva 2002/58, à luz dos artigos 7.°, 8.° e 52.°, n.º 1, da Carta, uma obrigação geral de conservar dados de tráfego relativos a todas as pessoas, a todos os meios de comunicação eletrónica e a todos os dados de tráfego, sem quaisquer distinções, limitações ou exceções, para efeitos do objetivo de combate à criminalidade [...]?

2) Em caso de resposta negativa à primeira questão, pode, não obstante, a conservação ser permitida quando:

a) o acesso das autoridades nacionais aos dados conservados seja determinado conforme [descrito nos n.ºs 19 a 36 da decisão de reenvio], e

b) [as exigências] de segurança sejam regulad[a]s conforme [descrito nos n.ºs 38 a 43 da decisão de reenvio], e

c) todos os dados relevantes sejam conservados pelo período de seis meses, calculado a partir do dia em que cessa a comunicação, sendo subsequentemente apagados conforme [descrito no n.º 37 da decisão de reenvio]?"[25]

Ao passo que no segundo processo foram mobilizadas como questões prejudiciais:

– "1) O acórdão [DRI] (incluindo, em especial, os seus n.ºs 60 a 62) estabelece exigências imperativas de direito da União, aplicáveis ao regime interno de um Estado-Membro que regula o acesso a dados conservados em conformidade com a legislação nacional, a fim de dar cumprimento aos artigos 7.° e 8.° da [Carta]?

25 Acórdão de 8 de abril de 2014 do TJUE, p. 18, disponível em https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A62015CJ0203 (consultado em 23.05.2022).

2) O acórdão [DRI] alarga o âmbito de aplicação dos artigos 7.º e/ou 8.º da Carta para além do âmbito de aplicação do artigo 8.º da [CEDH], tal como definido na jurisprudência do Tribunal Europeu dos Direitos do Homem [...]?"[26]

Neste aresto, o TJUE concluiu que:

– "O artigo 15.º, n.º 1, da 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), conforme alterada pela Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009, lido à luz dos artigos 7.º, 8.º e 11.º, bem como do artigo 52.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia, deve ser interpretado no sentido de que se opõe a uma regulamentação nacional que prevê, para efeitos de luta contra a criminalidade, uma conservação generalizada e indiferenciada de todos os dados de tráfego e dados de localização de todos os assinantes e utilizadores registados em relação a todos os meios de comunicação eletrónica.

2) O artigo 15.º, n.º 1, da Diretiva 2002/58, conforme alterada pela Diretiva 2009/136, lido à luz dos artigos 7.º, 8.º e 11.º bem como do artigo 52.º, n.º 1, da Carta dos Direitos Fundamentais, deve ser interpretado no sentido de que se opõe a uma regulamentação nacional que regula a proteção e a segurança dos dados de tráfego e dos dados de localização, em especial, o acesso das autoridades nacionais competentes aos dados conservados, sem limitar, no âmbito da luta contra a criminalidade, esse acesso apenas para efeitos de luta contra a criminalidade grave, sem submeter o referido acesso a um controlo prévio por parte de um órgão jurisdicional ou de uma autoridade administrativa independente, e sem exigir que os dados em causa sejam conservados em território da União.

3) A segunda questão submetida pela Court of Appeal (England & Wales) (Civil Division) [Tribunal de Recurso (Inglaterra e País de Gales) (Divisão Cível), Reino Unido] é inadmissível."[27]

---

26 Acórdão de 8 de abril de 2014 do TJUE, pp. 19 e 20, disponível em https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A62015CJ0203 (consultado em 23.05.2022).

27 Acórdão de 8 de abril de 2014 do TJUE, p. 31, disponível em https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A62015CJ0203 (consultado em 23.05.2022).

Como se infere, o TJUE considerou que a operação de conservação generalizada e indiferenciada dos dados de tráfego e dos dados de localização, referentes a todos os assinantes e utilizadores, ante todos os meios de comunicação, violava o direito ao respeito pela vida privada e familiar, além de consubstanciar também uma violação do direito à proteção dos dados pessoais, e ainda à liberdade de expressão, contidos nos artigos 7.º, 8.º e 11.º da Carta dos Direitos Fundamentais da União Europeia (doravante, Carta). De igual modo, o TJUE entendeu que o acesso, ou como se destacou acima, a transmissão de dados dos fornecedores de serviços aos órgãos de polícia criminal, sem prévio controlo jurisdicional, ou de uma autoridade administrativa independente, e sem exigência de conservação em território da UE, viola os mesmos direitos e liberdade fundamentais. Assinala-se que alguns dos reparos tecidos no acórdão em apreço não têm cabimento à luz do diploma nacional, conforme sinalizaremos adiante.

6. O acórdão de 21 de dezembro de 2016 do Tribunal de Justiça da União Europeia

Outra decisão jurisprudencial, mais relevante até e que viria a ter um impacto significativo na ordem jurídica nacional, ainda que não acolhida numa primeira fase pelo TC, foi proferida pelo TJUE, no âmbito de pedidos prejudiciais 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), movido contra Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Irlanda e The Attorney General.

Neste processo que abrangeu dois apensos – C-293/12 e C-594/12 – foram suscitadas, no primeiro, as questões prejudiciais que se transcrevem, a saber:

– "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 circularem e permanecerem 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)?"[28]

Ao passo que, no segundo apenso, delimitaram-se como questões prejudiciais:

– "1) Quanto à validade dos atos adotados pelas instituições da União: Os artigos 3.° a 9.° da Diretiva [2006/24] são compatíveis com os artigos 7.°, 8.° e 11.° da [Carta]?

2) Quanto à interpretação dos Tratados:

28 Acórdão de 21 de fevereiro de 2016 do TJUE, p. 13 disponível em https://eur-lex.europa.eu/legal-content/pt/TXT/?uri=CELEX%3A62012CJ0293 (consultado em 25.03.2022).

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?"[29]

E a propósito das questões prejudiciais acima transcritas, o TJUE considerou:

29 Acórdão de 21 de fevereiro de 2016 do TJUE, p. 14 disponível em https://eur-lex.europa.eu/legal-content/pt/TXT/?uri=CELEX%3A62012CJ0293 (consultado em 25.03.2022).

– "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."[30]A declaração de invalidade da Diretiva 2006/24/CE[31] tem por base a tradicional enumeração dos comandos europeus aplicáveis, bem como o direito ao respeito da vida privada e familiar, na medida em que a conservação dos dados de tráfego e de localização, por referentes à vida privada de uma pessoa e às suas comunicações, constitui *a se*, uma ingerência nos direitos fundamentais garantidos pelo artigo 7.º da Carta.

Por outro lado, estando em causa a conservação dos dados e a subsequente transmissão aos órgãos de polícia criminal nacionais configura, pois, uma ingerência no direito à proteção dos dados pessoais, vertido no artigo 8.º da Carta, por prever, pelo menos, duas operações de tratamento de dados pessoais distintas.

No essencial, o TJUE declarou a invalidade da Diretiva, convocando quatro argumentos distintos, reportando-se à violação dos direitos fundamentais em crise, como também à violação do princípio da proporcionalidade, nas suas dimensões de necessidade e de não excessividade ou proporcionalidade em sentido restrito. Impõe-se explicitar tais fundamentos.

Em primeiro lugar, a consideração de que a conservação dos dados de tráfego e de localização, referentes a todas as pessoas, de todas as comunicações, sem qualquer critério, colocando em paridade suspeitos e arguidos com as pessoas sobre as quais inexistam indícios cujos comportamentos possam ter alguma associação direta ou reflexa com infrações graves. Mais a mais,

30 Acórdão de 21 de fevereiro de 2016 do TJUE, p. 21 disponível em https://eur-lex.europa.eu/legal-content/pt/TXT/?uri=CELEX%3A62012CJ0293 (consultado em 25.03.2022).

31 Relativamente ao conceito de validade, é idêntico ao de legalidade e abrange tanto a legalidade interna, como a legalidade externa, cf. Ana Guerra Martins, *Manual de Direito da União Europeia*, 2.ª Edição, (Coimbra: Almedina, 2017), 576.

como assinala o TJUE, "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.".[32] Note-se que estava em causa a recolha massiva e indiscriminada dos dados de tráfego e de localização.

Em segundo lugar, a ausência de critérios objetivos na Diretiva que permitam delimitar a transmissão dos dados para as autoridades nacionais competentes, quedando-se pela fórmula normativa genérica e abstrata "crimes graves", a ser definido pelo direito interno dos Estados-Membros, associada à carência de densificação das condições materiais e processuais, fundamentaram o reparo do TJUE.

Em terceiro lugar, a falta de distinção dos prazos de conservação atinentes às categorias de dados plasmadas no artigo 5.º da Diretiva, acrescido dos prazos mínimo e máximo de conservação dos dados pessoais, não existindo qualquer critério objetivo que garanta que a operação de tratamento se limita ao estritamente necessário, permitiu ao TJUE propender para a ingerência ou restrição[33] aos conteúdos essenciais dos direitos fundamentais já referenciados, "[...] 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".[34]

---

32 Acórdão de 21 de fevereiro de 2016 do TJUE, p. 20 disponível em https://eur-lex.europa.eu/legal-content/pt/TXT/?uri=CELEX%3A62012CJ0293 (consultado em 25.03.2022).

33 Este conceito poderá ser definido como "[...] toda a compressão do âmbito de proteção do direito, traduzida na desconsideração de elementos do objeto de proteção, ou na recusa da titularidade ou exercício de meios jurídicos destinados à respetiva fruição, operada por ato do poder público de natureza geral e abstrata ou individual e concreta", José Manuel Sérvulo Correia, *O Direito de Manifestação, âmbito de proteção e restrições*, (Coimbra: Almedina, 2006), 61.

34 Acórdão de 21 de fevereiro de 2016 do TJUE, p. 20 disponível em https://eur-lex.europa.eu/legal-content/pt/TXT/?uri=CELEX%3A62012CJ0293 (consultado em 25.03.2022).

Nestes termos, o TJUE considerou que o legislador europeu exorbitou os limites resultantes do princípio da proporcionalidade, nas vertentes da necessidade e não excessividade, à luz dos direitos ao respeito pela vida privada e familiar e à proteção dos dados pessoais, vertidos no n.º 1 do artigo 52.º, artigo 7.º e artigo 8.º, todos da Carta e declarou a invalidade da Diretiva, a qual implica a nulidade *ipso jure* do diploma europeu.

7. O acórdão n.º 268/2022 do Tribunal Constitucional

Finalmente aqui chegados, importa centrarmo-nos no aresto nacional, não sem antes se expenderem algumas considerações prévias pertinentes.

Na sequência da prolação do acórdão acima apreciado sumariamente, a CNPD proferiu a deliberação n.º 641/2017, em que assinalou os argumentos referenciados pelo TJUE no aresto conhecido por Digital Rights, manifestando que o primeiro argumento contaminava igualmente a Lei n.º 32/2008, recomendando a revisão do diploma legal nacional[35], por um lado.

Por outro, a CNPD formulou algumas sugestões por forma a suprir a violação do princípio da proporcionalidade e dos direitos fundamentais contidos no n.º 1 do artigo 26.º e no artigo 35.º, ambos da CRP. O que bem se justificava, visto que a declaração de invalidade formaria um dever para os Estados-Membros de reavaliar os diplomas nacionais, em ordem a assegurar a compatibilidade com a Carta, mas também com as Constituições nacionais.

Na sequência de múltiplas participações provenientes do Ministério Público, de diversas comarcas do país, considerando as competências sancionatórias vertidas no n.º 1 do artigo 14.º da Lei n.º 32/2008, e face à declaração de invalidade da Diretiva proferida pelo TJUE, a CNPD proferiu nova deliberação, correspondente ao n.º 1008/2017, em que decidiu pela desaplicação da Lei n.º 32/2008[36], na sequência das situações que lhe fossem

35 Cf. deliberação, p. 5v, disponível em https://www.cnpd.pt/decisoes/historico-de-decisoes/?year=2017&type=2&ent= (consultada em 23.05.2022).

36 A este propósito importa notar que: "Na verdade, com vista à prossecução do objetivo de assegurar a primazia do Direito da União sobre os Direitos nacionais, o TJ impôs às autoridades dos Estados-membros um conjunto de deveres, dos quais se destacam:

submetidas para apreciação, em cumprimento do princípio do primado do Direito da União e da prevalência da Constituição.[37] A solução preconizada pela autoridade administrativa independente em causa foi, aliás, reconhecida e aceite pelo Acórdão 268/2022 do TC.[38] É evidente que tal deliberação correspondeu a um anúncio formal, visto que tal desaplicação seria operada nos processos que fossem espoletados junto daquela autoridade administrativa independente, individualizadamente, *i.e.*, processo a processo.

O processo de fiscalização da constitucionalidade que deu origem ao acórdão que seguidamente afloraremos resultou do pedido formulado pela Provedora de Justiça, tendente à apreciação e declaração, com força obrigatória geral, da inconstitucionalidade das normas constantes dos artigos 4.º (referente às categorias de dados), 6.º (atinente ao período de conservação) e 9.º (que se reporta à transmissão dos dados). O pedido fundamentou-se, em suma, na violação do princípio da proporcionalidade na restrição dos direitos à reserva da intimidade da vida privada e familiar (n.º 1 do art. 26.º da CRP), do sigilo das comunicações (n.º 1 do art. 34.º da CRP) e a uma tutela jurisdicional efetiva (n.º 1 do art. 20.º da CRP).

A propósito dos artigos 4.º e 6.º da Lei n.º 32/2008, a problemática apreciada pelo TC residiu na verificação dos pressupostos para a legitimidade constitucional da compressão dos direitos fundamentais à reserva da intimidade da vida privada, ao livre desenvolvimento da personalidade e à

– A não aplicação do Direito nacional incompatível;

– A interpretação conforme do Direito nacional com o Direito Comunitário (e hoje com o Direito da União Europeia);

- A supressão ou a reparação das consequências de um ato nacional contrário ao Direito Comunitário (e hoje ao Direito da União Europeia);

- O controlo jurisdicional efetivo da aplicação do Direito Comunitário (atualmente também com o Direito da União Europeia);

- Os Estados-membros devem fazer respeitar as regras comunitárias (e da União) pelos seus nacionais.

O Tribunal retirou do princípio do primado a ideia de que cabe tanto aos tribunais nacionais como às autoridades administrativas, incluindo a administração descentralizada do Estado, assegurar a aplicação integral do primado e conferir proteção aos direitos que antes o Direito Comunitário, e atualmente o Direito da União, atribuem aos particulares, não aplicando toda e qualquer norma nacional contrária.", Ana Guerra Martins, *Manual de Direito da União Europeia*, 2.ª edição, (Coimbra, Almedina, 2017), 522 e 523.

37 Cf. deliberação, p. 2, disponível em https://www.cnpd.pt/decisoes/historico-de-decisoes/?year=2017&type=2&ent= (consultada em 23.05.2022).

38 Cf. acórdão n.º 268/2022 proferido em Plenário, pelo Tribunal Constitucional, p. 22, disponível em https://www.tribunalconstitucional.pt/tc/acordaos/20220268.html (23.05.2022).

proteção de dados pessoais. Preferimos esta denominação, ante o direito à autodeterminação informativa, conceito empregue diversas vezes no acórdão em análise, mas não unânime na doutrina nacional e estrangeira. Todavia, por configurar matéria que se localiza à margem do objeto do presente artigo, não desenvolveremos essa temática.

Justifica-se, pois, perscrutar os principais argumentos, de forma sumária, que conduziram ao juízo efetuado pelo TC, bem como a ilação extraída.

O TC considerou que o legislador não prescreveu a necessidade do armazenamento dos dados de tráfego e de localização ocorrer no território da UE, colocando em crise os n.ºs 1 e 4 do artigo 35.º da CRP que contemplam o direito à proteção dos dados pessoais, visto que a possibilidade de armazenamento fora desse território coloca em crise a efetividade do exercício dos direitos de informação e de acesso, entre outros, dos titulares dos dados. Em face deste argumento, o TC concluiu pela inconstitucionalidade, por violação do direito à proteção dos dados pessoais, contido nos n.ºs 1 e 4 do artigo 35.º da Lei fundamental portuguesa, interpretado conforme o disposto nos artigos 7.º e 8.º da Carta, das normas referentes às categorias de dados e ao prazo de conservação, plasmadas nos artigos 4.º e 6.º da Lei n.º 32/2008.[39]

Depois, o TC entendeu igualmente, ante a conservação massiva dos dados de tráfego e de localização da totalidade da população, sem qualquer diferenciação, que a medida transpôs os limites ditados pelo princípio da proporcionalidade. Nesse sentido considerou-se uma vez mais como inconstitucionais, na interpretação conjugada dos artigos 4.º e 6.º, por violação dos n.ºs 1 e 4 do artigo 35.º e do n.º 1 do artigo 26.º, em conjugação com o n.º 2 do artigo 18.º da CRP.

A seguir, o TC reconheceu ainda que a ausência de notificação ao titular dos dados de eventuais acessos aos dados de tráfego e de localização restringia o direito à proteção dos dados pessoais, como também à tutela jurisdicional efetiva, consagrado no n.º 1 do artigo 20.º da CRP, por obstar "[...] a viabilidade prática de exercício de controlo judicial de acessos abusivos ou ilícitos

39 Cf. acórdão n.º 268/2022 proferido em Plenário, pelo Tribunal Constitucional, p. 40, disponível em https://www.tribunalconstitucional.pt/tc/acordaos/20220268.html (23.05.2022).

aos dados conservados".[40] Com este pressuposto, embora o TC tenha efetuado outras ponderações, declarou a inconstitucionalidade do artigo 9.º da Lei n.º 32/2008, na parte em que não prevê, em tais circunstancialismos, uma notificação ao visado, por violação do n.º 1 do artigo 35.º e do n.º 1 do artigo 20.º, em conjugação com o n.º 2 do artigo 18.º, todos da CRP.

Nestes termos, no campo da justiça constitucional entendeu-se, e a nosso ver bem, declarar a inconstitucionalidade, com força obrigatória geral, das normas contidas nos artigos 4.º, 6.º e 9.º da Lei n.º 32/2008, ainda que com alguns argumentos e convocando parâmetros de índole distinta, face àqueles que foram empregues pelo TJUE. A este propósito assinala-se como principais diferenças o argumento referente à obrigação de conservação dos dados pessoais no território da UE, como também o argumento referente ao direito à tutela jurisdicional efetiva, quanto à notificação dos titulares nas hipóteses de acesso abusivo ou ilícito. Tais fundamentos não foram objeto de apreciação pelo TJUE.

Por outro lado, compulsando a sentença proferida, o TC não efetuou nenhuma manipulação dos efeitos, restringindo-os. Pelo contrário, a declaração com força obrigatória geral da inconstitucionalidade das normas contidas nos artigos 4.º, 6.º e 9.º da Lei n.º 32/2008 implica a nulidade das mesmas, produzindo a sentença eficácia retroativa ou *ex tunc*. Sublinha-se que o n.º 3 do artigo 282.º da CRP contempla uma importante exceção ao princípio da intangibilidade do caso julgado.[41] O que determina que caberá aos condenados ou os seus defensores, salvo melhor opinião, a interposição do recurso de revisão (cf. al. *c*) do n.º 1 do art. 450.º do CPP, com fundamento na *f*) do n.º 1 do art. 449.º do CPP), ante a declaração, pelo Tribunal Constitucional, da inconstitucionalidade com força obrigatória geral das normas de conteúdo menos favorável ao arguido que tenham servido de fundamento à condenação. O que justificará uma apreciação, naturalmente, casuística e profunda. Tal apreciação reclamará a indagação das provas concretamente obtidas e utilizadas nos processos-crimes com sentenças ou acórdãos já transitados em

40 Cf. acórdão n.º 268/2022 proferido em Plenário, pelo Tribunal Constitucional, p. 54, disponível em https://www.tribunalconstitucional.pt/tc/acordaos/20220268.html (23.05.2022).

41 Cf. José Joaquim Gomes Canotilho**,** *Direito Constitucional e Teoria da Constituição*, 7.ª edição, (Coimbra, Almedina, 2003), 1015.

julgado e aquilatar da relevância probatória dos dados de tráfego e de localização para a construção do quadro factual dado como provado que suportou tais decisões penais. Sinaliza-se ainda que inexistia no ordenamento jurídico nacional diploma prévio ao ora apreciado, razão pela qual não opera o fenómeno da repristinação. Também salvo melhor opinião, não caberia ao TC determinar a revisão dos processos-crime na sentença proferida, contrariamente a algumas opiniões propaladas na comunidade jurídica nacional.

Outra consequência importante relaciona-se com as entidades fornecedoras de serviços de comunicações eletrónicas publicamente disponíveis, ou de uma rede pública de comunicações. Após o trânsito em julgado do acórdão em apreço e depois de publicado em Diário da República, tais entidades deverão proceder ao apagamento dos dados de tráfego e de localização conservados. Sublinhe-se que da sentença ressalta um efeito que a doutrina constitucionalista nacional associa às ideias de vinculação geral e de força de lei.[42] Em causa, está "[...] (i) vinculação geral, porque as sentenças do TC declarativas da inconstitucionalidade ou da ilegalidade vinculam – mas apenas quanto à parte dispositiva das decisões e não quanto aos seus fundamentos determinantes, ou seja, a *ratio decidendi* – todos os órgãos constitucionais, todos os tribunais e todas as autoridades administrativas; (ii) força de lei, porque as sentenças têm valor normativo (como as leis) para todas as pessoas físicas e coletivas (e não apenas para os poderes públicos) juridicamente afetadas nos seus direitos e obrigações pela norma declarada inconstitucional".[43] Do aresto promana diretamente a obrigação das entidades fornecedoras de serviços de comunicações eletrónicas publicamente disponíveis, ou de uma rede pública de comunicações, procederem ao apagamento dos dados de tráfego e de localização que, porventura, conservem.

Por fim, destaca-se ainda que o acórdão do TC foi, porém, objeto de duas declarações de voto, uma denominada "conjunta", ou como mera "declaração de voto". Note-se que apenas um Juiz Conselheiro votou contra a declaração de voto conjunta.[44]

42 Cf., por todos, *Ibidem*, 1009.

43 *Ibidem*, 1011.

44 Cf. acórdão n.º 268/2022 proferido em Plenário, pelo Tribunal Constitucional, p. 55, disponível em https://www.tribunalconstitucional.pt/tc/acordaos/20220268.html (23.05.2022).

A declaração de voto conjunta fundamenta-se, em síntese, na ausência de convocação do parâmetro jurídico-constitucional consagrado nos n.ºs 1 e 4 do artigo 34.º da CRP, por considerar que os artigos 4.º e 6.º da Lei n.º 32/2008, por atingir as pessoas "[...] que não estão, sequer remotamente, ligadas a qualquer processo criminal [...]", comando constitucional aquele que não foi aplicado no juízo de inconstitucionalidade das normas em causa, vertido na sentença.

Por outro lado, a declaração de voto subscrita por quase metade dos juízes conselheiros do TC, em que concordando com o resultado vertido no dispositivo do aresto, manifestam a divergência quanto à omissão do parâmetro do n.º 4 do artigo 8.º da CRP).[45] A par desta discordância que fundamenta substancialmente a referida declaração, milita outra na decorrência do antecedente, desta feita quanto à ausência de referência ao princípio da interpretação conforme ao Direito da União Europeia, estando também em causa o princípio da cooperação leal.

8. Conclusões sumárias

Aqui chegados assinala-se que a conservação e transmissão dos dados de tráfego e de localização não é uma problemática, como se constatou, dotada de cariz inovatório.

Aliás, os dois arestos europeus apreciados, sobretudo o segundo, já indiciavam, face aos parâmetros jurídico-europeus, dotados de valor constitucional, que as normas vertidas nos artigos 4.º, 6.º e 9.º da Lei n.º 32/2008 dificilmente seriam compatíveis com a CRP.

Acresce ainda que a problemática em apreço não mereceu da parte do legislador nacional a devida atenção, visto que se teria imposto a necessária revisão do diploma nacional, por forma a não enfermar dos vícios de inconstitucionalidade apontados no douto acórdão do TC. Mais a mais que o diploma foi até objeto de recentes alterações, através da Lei n.º 79/2021, de 24 de novembro, mais concretamente de aditamentos que não incidiram sequer sobre as normas fiscalizadas no aresto em causa.

45 Cf. acórdão n.º 268/2022 proferido em Plenário, pelo Tribunal Constitucional, p. 61, disponível em https://www.tribunalconstitucional.pt/tc/acordaos/20220268.html (23.05.2022).

Por outro lado, também não joga a favor, particularmente da Assembleia da República, o argumento de que as questões de inconstitucionalidade agora apreciadas e decididas não haviam sido manifestas tempestivamente, visto que, quer na comunidade jurídica nacional quer a CNPD, alertaram em diversas ocasiões para a necessidade de revisão do diploma, porém, sem acolhimento.

Outra conclusão relevante é não atribuir a denominação de "metadados" aos dados de tráfego e de localização, dado que são dados pessoais, não tendo aquele conceito guarida legal europeia ou nacional, ou doutrinal, constituindo uma criação jurisprudencial nacional.

Depois, em sede das presentes conclusões sumárias importará efetuar algumas modestas sugestões a propósito da nova lei que regule a conservação dos dados de tráfego e de localização.

Numa proposta metódica justifica-se identificar as principais problemáticas, para depois avançar com sugestões. Seguindo de perto o enunciado que antecede e ante as ilações que se extraíram quer da jurisprudência europeia quer da jurisprudência constitucional, permitem aduzir que uma medida legislativa de conservação dos dados de tráfego e de localização, massiva e indiscriminadamente, sem qualquer diferenciação, é uma das problemáticas a perpassar pelos arestos apreciados sumariamente. Outra assente na ausência de delimitação de critérios objetivos que sirvam de base à transmissão dos dados pessoais em causa às autoridades policiais – este pressuposto, reconheça-se, ainda foi objeto de mitigação por parte do legislador nacional. Depois, outra premissa relaciona-se com a falta de critérios objetivos que permitam mensurar a determinação do período de conservação dos dados de tráfego e de localização. Ora, também este pressuposto foi, em parte, mitigado, visto que foi estabelecido o prazo de 1 ano, e não o prazo máximo de 2 anos, permitido pela Diretiva 2006/24/CE.

Com base nestes pressupostos dir-se-á, até percorrendo lugares paralelos, relativamente à primeira premissa e bem sinalizado em *obiter dictum* pelo acórdão do TC, "[...] na base de dados de perfis de ADN, em que se não determinou a conservação de todos os dados de todos os cidadãos – mas apenas de um leque circunscrito de sujeitos (voluntários, pessoas condenadas em processo criminal; arguidos em processo criminal; etc. – artigo 15.º da

Lei n.º 5/2008, de 12 de fevereiro, na versão que lhe foi conferida pela Lei n.º 90/2017, de 22 de agosto). Ou, ainda, no regime estatuído pelo artigo 12.º da Lei do Cibercrime (Lei n.º 109/2009, de 15 de setembro), que plasma uma possibilidade de *quick-freeze*, admitindo que a autoridade judiciária (ou o órgão de polícia criminal, nos casos do n.º 2) requeira ao fornecedor do serviço a preservação e conservação dos dados determinados como necessários à produção da prova, a partir do momento em que é feito o pedido. Em contraste, nas normas fiscalizadas, consagrou-se uma solução que indiscutivelmente apresenta maior eficácia, abrangendo todos os dados de todos os utilizadores".[46]

Crê-se que deveriam ser empregues critérios objetivos, com uma delimitação normativa que aludisse a eventos de risco elevado, em que se proceda à conservação dos dados de tráfego e de localização dos assinantes e utilizadores registados nas áreas geográficas – preferencialmente nos concelhos em que tais eventos tivessem lugar. Por exemplo, eventos desportivos de elevado risco em matéria de segurança, visita de chefes de Estado estrangeiros, visita de altos representantes das religiões, entre outros. Desse modo, admite-se, assegurar-se-ia a necessidade e não excessividade de tal medida, compatibilizando-a com o direito à reserva da vida privada, com a inviolabilidade das comunicações e ainda com o direito à proteção dos dados pessoais.

Outrossim deveria ser consagrada a norma de que as entidades vinculadas à obrigação de conservação dos dados de tráfego e de localização o fariam em território da União Europeia, assegurando o exercício dos direitos dos titulares dos dados.

A par desta solução importaria ainda que os prazos de conservação dos dados pudessem ser fixos, ante as categorias de dados em causa, de forma assimétrica. Para tanto, sugere-se o prazo de 6 meses para os dados de tráfego e o prazo de 3 meses para os dados de localização. Tal opção fundamenta-se na circunstância de os dados de localização, por se afigurarem mais intrusivos ou impactantes da reserva da vida privada e na proteção de dados, justificarem um prazo mais curto. Sublinha-se que tal consideração tem por base uma panóplia de meios de prova admitidos, dado que no sistema jurídico-penal

46 Acórdão n.º 268/2022 proferido em Plenário, pelo Tribunal Constitucional p. 44, disponível em https://www.tribunalconstitucional.pt/tc/acordaos/20220268.html (23.05.2022).

nacional opera o regime da prova livre. Ademais, os prazos de conservação dos dados de conteúdo das comunicações são diversos dos ali propostos e seguramente mais relevantes probatoriamente para o apuramento da verdade material e para a realização da justiça penal.

Depois, ante a redação do artigo 9.º da Lei n.º 32/2008 e face aos pertinentes reparos tecidos pelo acórdão do TC, justifica-se a consagração de uma solução normativa que viabilize a constituição de um mecanismo de alarmística que permita a notificação do titular dos dados. Essa notificação deveria operar em circunstâncias que correspondam a eventual acesso abusivo ou ilícito por parte das autoridades de investigação criminal, sobretudo quando a comunicação não seja suscetível de comprometer as investigações criminais, nem os bens jurídicos como a vida ou a integridade física de terceiros.

Crê-se que estas medidas, entre outras, seriam idóneas e compatíveis com os parâmetros constitucionais nacionais, os quais foram mobilizados e legitimaram as decisões tomadas pelo TC sobre as questões de inconstitucionalidade, afigurando-se conformes à ordem constitucional de valores.

Em jeito conclusivo, uma última palavra para dar nota de que o douto acórdão do TC revela uma leitura novamente, e bem a nosso ver, mais rígida do texto constitucional vigente e garantística dos direitos fundamentais, em sentido contrário, ainda que não integralmente, ao acórdão n.º 464/2019, de 18 de setembro, proferido pelo TC, aquando da apreciação das questões de inconstitucionalidade suscitadas a propósito da Lei Orgânica n.º 4/2017, de 25 de agosto, que regula o acesso dos oficiais de informações do SIS e do SIED aos dados de telecomunicações e internet.