Metadados, direitos fundamentais e o novo regime português

Beatriz Assunção Ribeiro
Associada, VdA
bea@vda.pt

Iakovina Kindylidi
Senior International Advisor, VdA
imk@vda.pt

Resumo:
Na sequência do Acórdão Digital Rights Ireland do Tribunal de Justiça da União Europeia e do Acórdão n.º 268/2022 do Tribunal Constitucional, o regime dos metadados tem sido objeto de discussão nos últimos anos, da qual resultou a aprovação de um novo regime a este respeito. Este artigo visa sobretudo discutir e explicar os conceitos básicos associados à temática dos metadados, bem como analisar algumas questões associadas ao regime entretanto aprovado em Portugal.

Palavras-chave:
PT: Metadados, privacidade, segurança, direitos fundamentais
EN: Metadata, privacy, security, fundamental rights

1. INTRODUÇÃO

Em qualquer comunicação é possível distinguir entre o seu conteúdo, isto é, a informação propriamente dita que essa comunicação pretende transmitir, e uma série de outros elementos que envolvem essa

comunicação, que a delimitam (no espaço e no tempo) e lhe dão suporte[1]. Estes elementos são comummente descritos como *dados sobre dados* – metadados – e incluem informação sobre, por exemplo, a localização de emissão dessa comunicação, o seu tempo, e a sua origem e destino. Em suma, os metadados correspondem a toda informação que pode ser recolhida a respeito de uma comunicação, que não seja o próprio conteúdo em si.

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, e que altera a Diretiva 2002/58/CE ("Diretiva 2006/24") visava harmonizar as disposições dos EstadosMembros relativas à conservação de determinados dados gerados ou tratados pelos fornecedores de serviços de comunicações eletrónicas, procurando garantir a disponibilidade desses dados para efeitos de investigação, de deteção e de repressão de infrações graves, tais como crime organizado e terrorismo, no respeito dos direitos consagrados nos arts. 7.° e 8.° da Carta dos Direitos Fundamentais da União Europeia ("CDFUE").

Face às necessidades de uma década marcada por eventos trágicos no que respeita ao terrorismo e à necessidade urgente de se combater esta realidade, esta Diretiva nunca foi verdadeiramente colocada em causa até 2014, momento em que o Tribunal de Justiça da União Europeia ("TJUE") declarou a sua invalidade, no Acórdão Digital Rights Ireland[2].

---

[1] Acórdão n..º 403/2015, § 9, associado ao processo n..º 773/15, cujo relator é Conselheiro Lino Rodrigues Ribeiro, disponível em https://www.tribunalconstitucional.pt/tc/acordaos/20150403.html

[2] Tribunal de Justiça da União Europeia, Digital Rights Ireland Ltd contra Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Irlanda, datado de 8 de abril de 2014, processos apensos C293/12 e C594/12, disponível em https://curia.europa.eu/juris/document/document.jsf;jsessionid=3CE25888D6478AA3CC9ED7B78735A64F?text=&docid=150642&pageIndex=0&doclang=pt&mode=req&dir=&occ=first&part=1&cid=2712231

Neste seguimento, o tema dos metadados sofreu um revés significativo, gerando uma incerteza que dura até aos dias de hoje. Ainda que novas leis tenham sido aprovadas, um pouco por toda a Europa, com a missão de resolver as questões levantadas pelo TJUE no Acórdão, não é totalmente evidente se as soluções encontradas são definitivas e suficientes.

Ora, com a declaração da invalidade da Diretiva 2006/24, o enquadramento europeu relativamente a esta matéria voltou à base, isto é, à Diretiva 2002/58/CE do Parlamento e do Conselho, de 12 de julho, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas, mas também à CDFUE, que serve de pano de fundo interpretativo a toda a questão dos metadados, especialmente nos seus arts. 7.º (Respeito pela vida privada e familiar), 8.º (Proteção de dados pessoais), 11.º (Liberdade de expressão e de informação) e, na interpretação que lhes deve ser dada e compatibilização, quando necessária, o 52.º (Âmbito e interpretação dos direitos e dos princípios).

Concretamente em Portugal, este enquadramento era feito, mesmo após a declaração de invalidade da Diretiva 2006/24 pelo TJUE, pela Lei n.º 32/2008, de 17 de julho, sobre a conservação de dados gerados ou tratados no contexto oferta de serviços de comunicações eletrónicas ("Lei n.º 32/2008"). Eventualmente, os arts. 4.º (Categorias de dados a conservar), 6.º (Período de conservação) e 9.º (Transmissão dos dados) da Lei n.º 32/2008 acabaram declarados inconstitucionais, ainda que só em 2022, pelo Acórdão n.º 268/2022[3] do Tribunal Constitucional ("TC")[4].

Não se deve, contudo, olvidar que este não é o único enquadramento que pode ser feito a este respeito, o que significa que, mesmo

[3] Acórdão n..º 286/22, a respeito do processo n..º 828/2019, cujo relator é Conselheiro Afonso Patrão, disponível em https://www.tribunalconstitucional.pt/tc/acordaos/20220268.html

[4] De referir a este respeito que, apesar da Lei n..º 32/2008 em si mesma não ter sido considerada inconstitucional, é notório que os artigos afetados constituíam o verdadeiro núcleo do regime jurídico aqui em causa, e, sem eles, não era possível retirar-se qualquer consequência prática.

após o TC ter invalidado os artigos acima escritos, continuava a existir um enquadramento legal (ainda que parcial ou noutros termos) para os metadados. Efetivamente, as seguintes leis também se pronunciam sobre o assunto (com um âmbito mais ou menos restrito):

a. Lei n.º 109/2009, de 15 de setembro ("Lei do Cibercrime");
b. Lei n.º 41/2004, de 18 de agosto, sobre a proteção de dados pessoais e privacidade nas telecomunicações que transpôs a Diretiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de julho[5] ("Lei n.º 41/2004");
c. Lei Orgânica n.º 4/2017, de 25 de agosto, sobre o acesso dos oficiais de informações do SIS e do SIED a dados de telecomunicações e internet.

O presente artigo visa sobretudo analisar e explicar os conceitos básicos associados à temática, bem como analisar algumas questões associadas ao regime entretanto aprovado em Portugal.

2. QUESTÃO DE FUNDO E TIPOS DE METADADOS

À data da aprovação de qualquer declaração ou convenção dos direitos do homem, incluindo a europeia, bem como da Constituição da República Portuguesa ("CRP"), não existiam estes dispositivos eletrónicos que, hoje, nos seguem para todo o lado e constituem uma verdadeira extensão e materialização da nossa personalidade e consequentemente da nossa liberdade individual[6]. Mesmo as primeiras formas de telecomunicação criadas pela humanidade serviam tão-só para

[5] Uma pequena nota para destacar que esta lei, contrariamente à Lei n..º 32/2008, estabelece a possibilidade de os prestadores de serviços e comunicações eletrónicas conservarem certos tipos de dados mas não estabelece uma verdadeira obrigação.

[6] A única exceção a esta circunstância é, de facto, a CDFUE, que, proclamada pela primeira vez em 2000, já incluiu uma disposição específica relativa à proteção de dados pessoais (art. 8..º).

telecomunicar – i.e. expressar pensamentos por via telegráfica – mas não constituiam, na íntegra, um depósito portátil de cada ser humano como ocorre nos dias de hoje.

É esta a evolução que justifica que, em particular, o art. 34.º da CRP (Inviolabilidade do domicílio e da correspondência) seja lido a uma outra luz na era digital. É que a correspondência, que podia, à data da aprovação da CRP, corresponder a um mero reflexo esbatido da personalidade humana, revela hoje muito mais dessa personalidade do que alguma vez foi possível.

De facto, como bem refere o TJUE, a propósito de certos tipos de metadados, estes são hoje "suscetíveis de permitir tirar conclusões muito precisas sobre a vida privada das pessoas cujos dados foram conservados, como os hábitos da vida quotidiana, os lugares onde se encontram de forma permanente ou temporária, as deslocações diárias ou outras, as atividades exercidas, as relações sociais e os meios sociais frequentados"[7]. É precisamente por este motivo que estes dados são tão valiosos – porque a sua obtenção, no âmbito da investigação criminal, pode traduzir-se em avanços significativos nessa mesma investigação.

Ora, isto significa que qualquer ingerência que pudesse existir na correspondência, há cinquenta anos e no seu sentido literal de *correspondência*, não tem, nem pode ter, o significado atual: a ingerência nestas comunicações é, de forma inevitável, substancialmente mais grave.

Deste modo, a questão basilar e de fundo quanto ao tema dos metadados é essencialmente uma: a de concretizar o significado de correspondência e, deste modo, identificar o tipo de (meta)dados que, além do conteúdo, evidentemente abrangido pelo art. 34.º da CRP, fazem parte do núcleo duro deste direito constitucionalmente protegido

[7] Tribunal de Justiça da União Europeia, Digital Rights Ireland Ltd contra Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Irlanda, § 27, datado de 8 de abril de 2014, processos apensos C293/12 e C594/12, disponível em https://curia.europa.eu/juris/document/document.jsf;jsessionid=3CE25888D6478AA3CC9ED7B78735A64F?text=&docid=150642&pageIndex=0&doclang=pt&mode=req&dir=&occ=first&part=1&cid=2712231

que é o da inviolabilidade da correspondência. Por outras palavras, que interpretação deve ser dada, à luz dos tempos em que vivemos, ao referido artigo, e de que forma deve ser alargado o significado de correspondência para abranger os dados que orbitam o conteúdo da correspondência propriamente dito?

Nem todos, como veremos, pertencerão a este leque privilegiado de dados que, pela ingerência na vida privada e interferência na personalidade que qualquer acesso[8] permitiria, acesso este que seria insuportável num estado de Direito democrático, são (relativamente) invioláveis.

É por este motivo que a primeira distinção que os tribunais portugueses fazem a este respeito, e que tem vindo a ser repetida decisão após decisão, decorre de uma classificação tripartida dos dados envolvidos em qualquer comunicação: (a) dados de conteúdo, (b) dados de base e (c) dados de tráfego. Esta distinção já se encontra estabelecida em Portugal há mais de duas dezenas de anos tendo tal discussão tido lugar Acórdão n.º 241/2002, de 29/05/2002, sendo que já antes, em 07.07.1994, a Procuradoria-Geral da República se havia pronunciado sobre o tema, no seu Parecer n.º 16/1994[9]. Esta noção tripartida foi posteriormente acolhida pelo TC, sendo utilizada até aos dias de hoje.

Esta classificação tripartida diz-nos que:

a. **Dados de conteúdo:** os dados de conteúdo, como o próprio nome indica, tratam-se de dados relativos ao próprio conteúdo da mensagem, da correspondência enviada através da utilização da rede. Não são metadados propriamente ditos, constituindo antes o cerne da mensagem. A conservação e acesso ao conteúdo de qualquer carta, mensagem ou forma de comunicação tem um

[8] De notar, contudo, que, pelo menos no mundo digital, conservação dos dados, em si mesma, é naturalmente uma ingerência a estes direitos e é por isto que a questão se coloca logo à partida, antes do próprio acesso aos mesmos dados, que é uma derrogação muito mais intensa do que a simples conservação e que, por isso, está sujeita, pelo menos na Europa, a regras muito restritas.

[9] Disponível em https://www.ministeriopublico.pt/pareceres-pgr/8715

impacto de tal modo intolerável na personalidade e liberdade humana que dificilmente se poderia aceitar uma compatibilização com outros interesses, sem mais[10] e por este motivo tem um regime especialíssimo relativamente ao restante (veja-se, por exemplo, o regime aplicável às escutas telefónicas).

b. Dados de base: os (meta)dados de base dizem respeito à conexão à rede e que são, do ponto de vista operacional, necessários para utilização própria do respetivo serviço, dizendo respeito aos dados através dos quais o utilizador tem acesso ao serviço. Dados de base são caracteres permanentes, tais como o número de telefone, pelo que a identificação do sujeito a que pertencem pode ser obtida independentemente de qualquer comunicação. Correspondem, de certa forma, à nossa identificação no âmbito das comunicações.

c. Dados de tráfego: Por fim, quanto aos (meta)dados de tráfego, são os dados considerados necessários ao estabelecimento de uma ligação ou comunicação e os dados gerados pela utilização da rede para essa finalidade. São exemplos a localização do utilizador, localização do destinatário, duração da utilização, data e hora, frequência, dados de tráfego, necessários ou produzidos pelo estabelecimento da ligação da qual uma comunicação concreta é operada ou transmitida. Constituem elementos inerentes à própria comunicação, na medida em que permitem identificar, em tempo real ou *a posteriori*, os utilizadores, o relacionamento direto entre uns e outros através da rede, a localização, a frequência, a data, hora e a duração da comunicação.

---

[10] Como aliás explicita o TJUE no Acórdão Digital Rights Ireland "No que respeita ao conteúdo essencial do direito fundamental ao respeito da vida privada e dos outros direitos consagrados no art. 7.º da CDFUE, deve observarse que, embora a conservação dos dados imposta pela Diretiva 2006/24 constitua uma ingerência particularmente grave nesses direitos, não é suscetível de afetar o referido conteúdo, tendo em conta que, como resulta do seu art. 1.º, n.º 2, esta diretiva não permite tomar conhecimento do conteúdo das comunicações eletrónicas, enquanto tal".

Simplisticamente falando, se aquilo que se consegue retirar através de uma determinada informação for o conteúdo da mensagem – estaremos perante um dado de conteúdo; se o que é possível retirar da informação em causa é a identificação do utilizador que a origina – neste caso tratar-se-á de um dado de base; se está em causa qualquer informação que localize no tempo, no espaço e na rede aquela mensagem – então será um dado de tráfego[11].

De todo o modo, é curioso ver que, embora não seja totalmente claro de onde surgiu esta noção tripartida dos dados de uma comunicação, que dura até hoje, parece ter tido origem em doutrina francesa ou belga. Efetivamente, sem referenciar concretamente a fonte, o Parecer n.º 16/1994 menciona apenas que tal noção tripartida teve origem em Yves Poullet, reputado jurista belga, e Françoise Warran. Contudo, nem em França[12] nem na Bélgica[13], esta terminologia é utilizada, nem tão-pouco o TJUE faz uso dela, uma vez que não é utilizado pela legislação da UE, nem por outras legislações nacionais, pelo que é difícil identificar verdadeiramente origem desta noção tripartida.

Existem vários motivos que podem justificar esta circunstância, mas poderá estar relacionada com o facto de a divisão entre estas três categorias não ser totalmente linear. Com efeito, há casos em que um dado de base, pode ser simultaneamente um dado de tráfego, como ocorre, por exemplo, com o *Internet Protocol address* ("IP") e a localização.

---

[11] Note-se, claro, a bem do rigor científico, que estas se tratam de definições iminentemente práticas, porque a lei, na realidade, oferece definições teóricas destes conceitos, no art. 2..º, n..º 1 da Lei n..º 41/2004, de 18 de Agosto (Lei da Proteção de dados pessoais e privacidade nas telecomunicações).

[12] Em França, atualmente, os metadados são também denominados *donnés de connexion* que depois são subdivididos em cinco categorias: identidade (*Identité civile*), dados de contato e pagamento, dados relacionados a contratos e contas (*coordonnées de contact et de paiement, données relatives aux contrats et aux comptes*), endereços IP e equivalentes (*adresses IP et équivalents*), outros dados de tráfego e de localização (*autres données de trafic et données de localisation*); ver a este propósito o art. L34--1 do Código dos Correios e Comunicações Eletrónicas (*Code des postes et des communications électroniques*) e o relatório legislativo do senado a este propósito, disponível em https://www.senat.fr/rap/l20-694/l20-6946.html.

[13] Na Bélgica, os metadados a serem conservados estão listados no art. 126 da Lei relativa às comunicações eletrónicas, não sendo, de todo, agrupados em categorias.

A localização, como melhor explicado no Acórdão n.º 403/2015 do TC, diz respeito a *"dados tratados numa rede de comunicações eletrónicas que indiquem a posição geográfica do equipamento terminal de um utilizador de um serviço de telecomunicações, podendo incidir sobre a latitude, longitude ou altitude do equipamento, sobre a direção da deslocação, sobre a identificação da célula de rede em que o equipamento está localizado em determinado momento e sobre a hora de registo da informação de localização"*[14].

Ora, o TC, reconduzindo este conceito às categorias de metadados reconhecidas pelo próprio, defende que a informação relativa à localização (de um equipamento) pode enquadrar-se nos dados de base – quando identifica a posição geográfica do aparelho, independentemente de qualquer comunicação – ou nos dados de tráfego – quando esta identificação está associada a uma comunicação ou tentativa de comunicação. Ainda assim, o TC também argumenta, no Acórdão n.º 464/2019, que a primeira espécie dos dados de localização (a que não pressupõe comunicações em específico) é residual e que, por essa razão, tais dados de localização estão também incluídos no conceito mais amplo de *dados de tráfego*.

Esta posição baseou-se no parecer da Comissão Nacional de Proteção de Dados n.º 38/2017[15], que sustenta que, atualmente, ocorrem comunicações mesmo quando o utilizador do equipamento de comunicação não o aciona direta e intencionalmente, dando como exemplo o caso das atualizações efetuadas pelas aplicações de correio eletrónico ou outro tipo de mensagens, o que significa que a geração e troca de dados são praticamente constantes, mesmo quando os cidadãos utilizadores dos equipamentos nada fazem.

Em abstrato, esta justificação parece insuficiente para descartar, sem mais, a inclusão do dado *localização* – também – na categoria

[14] Acórdão n..º 403/2015, § 9, associado ao processo n..º 773/15, cujo relator é Conselheiro Lino Rodrigues Ribeiro, disponível em https://www.tribunalconstitucional.pt/tc/acordaos/20150403.html

[15] Parecer da Comissão Nacional de Proteção de Dados, a respeito do processo n..º 8243/2017, disponível em https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/105708

de dado de base, porque o facto de a geração e troca de dados ser constantes, sem necessidade de existência de envio de comunicações, não impede que (a) paralelamente, processos de identificação da localização, para outros efeitos, estejam a decorrer, nem que (b) num dado momento, ainda que temporalmente muito limitado, não existam comunicações a decorrer.

De resto, e embora criticável, de referir que também a doutrina portuguesa tem considerado que a localização está incluída, tal como o IP, no conceito mais amplo de dados de tráfego[16].

De facto, também o IP é uma questão controvertida, como bem mencionou o TC no Acórdão n.º 268/22, uma vez que pode não ter sempre a mesma qualificação. Os protocolos IP podem ser estáticos, o que significa que identificam, de forma permanente, um ponto de acesso à rede, ou dinâmicos, na medida em que são atribuídos a um certo dispositivo, no momento em que este faz a ligação à rede e apenas durante essa ligação. Por outras palavras, um protocolo IP dinâmico envolve informação da sua utilização num determinado momento, revelando informação sobre o utilizador, mas também sobre o uso da Internet num contexto específico.

Por este motivo, o Tribunal Constitucional Federal Alemão[17], entendeu que a identificação do titular de um protocolo IP dinâmico, ao pressupor uma consulta do tráfego para identificar o utilizador em dado momento, se enquadra nos dados de tráfego.

É esta a razão que justifica que também o TJUE muitas vezes analise autonomamente este tipo de dados[18]. Contudo, esta postura não foi acolhida pelo TC português no Acórdão n.º 268/22, que decidiu considerar o IP um dado base em qualquer circunstância.

---

[16] Veja-se, por exemplo, Catarina Sarmento e Castro, *Direito da Informática, Privacidade e Dados Pessoais*, Almedina, 2005, pág. 181.

[17] Acórdão do Tribunal Constitucional Alemão (Bundesverfassungsgericht – BVerfG), de 17 de julho de 2020, 1 BvR 1873/13 – 1 BvR 2618/13, §§ 101 e 102.

[18] Veja-se, por exemplo, o acórdão do Tribunal de Justiça da União Europeia, Tele2 Sverige AB contra Post och telestyrelsen, datado de 21 de dezembro de 2016, processo C203/15, disponível em https://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=5157465.

Subjacente a esta posição reside a ideia de que *ainda que seja discutível a respetiva categorização* – uma vez que o apuramento do endereço de protocolo IP dinâmico pressupõe a análise do momento em que se realizou uma concreta comunicação – *a intensidade de agressão aos direitos à reserva da intimidade da vida privada e à autodeterminação informativa é similar ao dos demais dados de base,* não relevando, no entender do TC, *as circunstâncias da comunicação, a sua duração, a pessoa com quem se comunica ou os sites consultados; limita-se a identificar, tal como nos demais dados de base, o utilizador daquele computador.*

O TC sustenta ainda esta posição dizendo que tal conclusão é congruente com a orientação defendida pelo TJUE, no Acórdão *La quadrature du net*, quando este refere que *"*os endereços IP, apesar de fazerem parte dos dados de tráfego, são gerados sem estarem ligados a uma comunicação específica e servem principalmente para identificar (…) a pessoa singular proprietária de um equipamento terminal a partir do qual é efetuada uma comunicação através da Internet. Assim, em matéria de correio eletrónico e de telefonia através da Internet, desde que apenas sejam conservados os endereços IP da fonte da comunicação e não os do seu destinatário, esses endereços não revelam, enquanto tais, nenhuma informação sobre terceiros que tenham estado em contacto com a pessoa que está na origem da comunicação. Por conseguinte, esta categoria de dados tem um grau de sensibilidade menor que o dos outros dados de tráfego*"* [19].

Não parece ser totalmente clara esta ligação que é feita entre a semelhança da lesão nos direitos fundamentais que decorre da conservação e acesso a um dado de base e a natureza do próprio metadado. Ou seja, o TC parece utilizar o facto de uma lesão entre a utilização

[19] Acórdão do Tribunal de Justiça da União Europeia, Quadrature du net e outros contra Premier ministre, Ministère de la Culture, datado de 6 de outubro de 2020, § 152, processos apensos C511/18, C512/18 e C520/18, disponível em https://curia.europa.eu/juris/document/document.jsf?text=&docid=232084&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=5163305

de dados de base ser uma – e o facto de no caso dos endereços de IP a lesão ser semelhante – para depois contrariar o TJUE (que diz expressamente que o endereço IP é um dado de tráfego, tal como descrito no parágrafo anterior) argumentando que é um dado de base.

É que, a acrescer à diferença entre endereços IP estáticos/dinâmicos, melhor descrita acima, apesar de identificar o dispositivo – e, portanto, poder considerar-se um dado de base – o endereço IP está também presente no momento do envio ou da receção da comunicação, não podendo esta ser separada daquele. Isto significa que, pelo menos até determinado ponto, o endereço IP caracteriza a própria comunicação e esta não pode ocorrer, num dado momento, sem aquele. Em suma, concluir pelo enquadramento do IP como dado de base não tem real justificação, com a consequência, como veremos, da consagração de uma proteção menor a este tipo de dados.

No final, é difícil não concluir que esta distinção é mais prejudicial do que propriamente benéfica, sobretudo porque – face à confusão que se gera com esta classificação – acaba por ter muito pouca relevância prática.

De facto, levanta-se a questão de se saber a verdadeira utilidade da distinção quando, em primeiro lugar, e por um lado, como já foi referido, nem todos os metadados em causa se enquadram numa ou noutra categoria, o que significa que esta distinção levanta mais questões do que as que resolve.

Por outro lado, o próprio regime jurídico aplicável não parece retirar consequências práticas desta distinção, sem prejuízo de o TC o ter feito, conferindo mais ou menos proteção conforme o tipo de dados em causa. Na prática, e nomeadamente em Portugal, e noutros outros ordenamentos jurídicos tal como em França, ocorria que os metadados são listados e o seu regime é tipicamente definido em bloco[20], como aliás refere o próprio TC no Acórdão n.º 403/2015

[20] Salvo uma ou outra exceção específica, por exemplo para efeitos de determinação do prazo de conservação, como ocorre em França.

quando refere que "é nesse sentido que a Lei n.º 32/2008, de 17 de julho, que regula a conservação e transmissão dos dados de tráfego e de localização, reserva a mesma disciplina jurídica para ambos"[21].

De resto, a própria Lei n.º 32/2008, identicamente à Diretiva 2006/24, distinguia entre:

a. Dados necessários para encontrar e identificar a fonte de uma comunicação;
b. Dados necessários para encontrar e identificar o destino de uma comunicação;
c. Dados necessários para identificar a data, a hora e a duração de uma comunicação;
d. Dados necessários para identificar o tipo de comunicação;
e. Dados necessários para identificar o equipamento de telecomunicações dos utilizadores, ou o que se considera ser o seu equipamento;
f. Dados necessários para identificar a localização do equipamento de comunicação móvel.

Ora, em nenhum momento parece decorrer esta distinção entre dados de base e dados de tráfego. Ocorre que, desta ficcionada distinção, conforme ficará patente na próxima secção, é de onde se retira a intensidade da proteção atribuída a cada uma das categorias como fez o Acórdão n.º 268/22 do TC.

3. A INGERÊNCIA NOS DIREITOS FUNDAMENTAIS

Como descreve o TC, "o direito ao livre desenvolvimento da personalidade abrange a faculdade de comunicar com segurança,

[21] Acórdão n..º 403/2015, § 9, associado ao processo n..º 773/15, cujo relator é Conselheiro Lino Rodrigues Ribeiro, disponível em https://www.tribunalconstitucional.pt/tc/acordaos/20150403.html

enquanto parte da sua liberdade de ação e de realização pessoal"[22]. É neste contexto também que se pode falar de um *direito à autodeterminação comunicativa* que se assume, também, como um direito de liberdade para comunicar, sem receio de que a comunicação ou as circunstâncias em que a mesma é realizada possam ser investigadas ou divulgadas.

Assim, mais do que uma questão intimamente relacionada com a privacidade propriamente dita, este direito demonstra-se de absoluta importância uma vez que, sem esta confiança, "o indivíduo sentir-se-á coartado na liberdade de poder comunicar com quem quiser, quando quiser, pelo tempo que quiser e quantas vezes quiser. Deste modo, é um direito que assegura o livre desenvolvimento das relações interpessoais e, ao mesmo tempo, de proteger a confiança que os indivíduos depositam nas suas comunicações privadas e no prestador de serviços das mesmas".

Como vimos, ainda que a distinção entre *dados de base e dados de tráfego* tenha relevância quase meramente teórica, o certo é que o TC faz uso da mesma para determinar que uma destas categorias – os dados de tráfego – merece proteção constitucional ao abrigo do art. 34.º da CRP e a restante categoria – dados de base – fica fora do âmbito de proteção do mesmo artigo[23].

É importante notar-se que o facto de os dados incluídos numa determinada categoria não estarem enquadrado no art. 34.º da CRP, não significa que não tenham respaldo constitucional. Efetivamente, não

---

[22] Acórdão n..º 403/2015, § 12, associado ao processo n..º 773/15, cujo relator é Conselheiro Lino Rodrigues Ribeiro, disponível em https://www.tribunalconstitucional.pt/tc/acordaos/20150403.html

[23] Esta é, de resto, jurisprudência reiterada do TC, que já havia explicado esta circunstância nos Acórdãos n..º 486/2009, 403/2015 e 463/2019. Neste contexto, nem todos os dados a que se refere o art. 4..º da Lei n..º 32/2008 estão protegidos pelo disposto nos números 1 e 4 do art. 34..º da Constituição. De acordo com a jurisprudência reiterada do TC, aquele parâmetro abrange os dados de tráfego quando pressuponham uma comunicação entre pessoas, mas já não os dados que, independentemente de qualquer comunicação, sejam atinentes à conexão de certo equipamento a uma rede de comunicações ou à mera identificação de um utilizador a quem estava atribuído um determinado número de telefone ou um endereço de protocolo IP estático; nem os dados de tráfego gerados pela comunicação entre um sujeito e uma máquina – v. g., a consulta de sítios da internet.

deixam de ter cabimento no art. 26.º da CRP, que diz respeito à reserva da intimidade privada[24], ainda que acoplado a esta circunstância venha, conforme referido pelo TC, um nível de proteção menos intenso do que aquele que o art. 34.º concede.

Na prática, esta distinção revela-se na ingerência que para a doutrina e jurisprudência é admissível num e noutro caso, que se traduz no entendimento comum de que uma determinada compressão dos direitos associados aos dados de base é aceitável, enquanto essa mesma compressão no caso dos dados de tráfego – que têm o potencial de revelar não apenas o utilizador como também a utilização da internet num determinado contexto – já não o será.

As ingerências em causa, por sua vez, e relativamente a dados de base e dados de tráfego, são a conservação (por determinado período e em determinado local) e o acesso. É relativamente a cada um destes regimes que o TC faz a sua análise.

É evidente que nos encontramos perante um caso paradigmático de ponderação e valores, e sobretudo de necessidade de compatibilização de direitos. Se, por um lado, temos este direito à reserva da intimidade privada (art. 26.º da CRP), de onde decorre também a inviolabilidade da correspondência (art. 34.º da CRP), por outro, temos o direito à segurança, também com previsão constitucional (art. 27.º da CRP).

Esta factualidade é relevante porque significa que qualquer acesso a metadados não se trata de uma ingerência sem mais, tratando-se antes de um importante processo de compatibilização de dois direitos fundamentais. E, portanto, como refere o Acórdão n.º 420/2017 do TC, a questão que se coloca é a de se aferir se a obrigatoriedade de os

[24] A este respeito, é também interessante referir que o TC, tal como melhor descreve no Acórdão n..º 403/2015, servindo-se da doutrina desenvolvida por Joaquim Sousa Ribeiro (em *A Tutela de bens da Personalidade na Constituição e na Jurisprudência constitucional portuguesas*, in Estudos de homenagem ao Prof. Doutor José Gomes Canotilho, Vol. III, Coimbra Editora, pág. 853) considera incluídos no art. 26..º da CRP outros direitos como, além da autodeterminação informacional, o direito à solidão e ao anonimato, bem como que todos estes direitos pesam na concretização da efetiva tutela constitucional a atribuir a estes dados.

fornecedores de serviços de comunicações eletrónicas conservarem este tipo de dados, constitui uma restrição destes direitos fundamentais e se tal restrição é desproporcionada nos termos do art. 18.º da constituição. Posto isto, é claro que não existem grandes dúvidas sobre a necessidade ou não de restrição dos direitos fundamentais em análise, mas antes sobre a sua proporcionalidade.

O princípio da proporcionalidade, como aliás sublinhado no Acórdão n.º 420/2017 do TC trata-se de um crivo basilar no plano das restrições de direitos fundamentais. De acordo com o n.º 2, do art. 18.º da Constituição, qualquer restrição "deve limitar-se ao necessário para salvaguardar outros direitos e interesses constitucionalmente protegidos". Por sua vez, assume três ramificações que constituem, na prática, critérios para aferir se determinada restrição passa ou não no crivo de proporcionalidade: (i) necessidade, (ii) adequação e (iii) proporcionalidade em sentido estrito.

Ora, para o TC é inequívoco que, relativamente aos dados de base, face ao interesse público prosseguido (i.e. investigação, deteção e repressão de crimes graves por parte das autoridades competentes, tal como previsto no art. 1.º, n.º 1, da Lei n.º 32/2008), tendo a "salvaguarda da legalidade democrática e a ação penal, nomeadamente contra os crimes referidos" interesse público e proteção constitucional"[25], a obrigação de os fornecedores de serviços de comunicações eletrónicas conservarem os dados de base cumpre os requisitos de necessidade[26], adequação e proporcionalidade em sentido estrito.

Em primeiro lugar porque, alega o TC, no Acórdão n.º 420/2017[27] "a conservação de dados de base é uma medida adequada para

[25] Acórdão n..º 420/2017, § 13, associado ao processo n..º 917/16, cujo relator é Conselheira Maria de Fátima Mata-Mouros, disponível em TC > Jurisprudência > Acordãos > Acórdão 420/2017. (tribunalconstitucional.pt).

[26] Aliás, como referiu o Conselho de Justiça e Assuntos Internos de 19 de dezembro de 2002, os dados relativos ao uso das comunicações eletrónicas são particularmente importantes e, portanto, uma ferramenta valiosa na prevenção de infrações e no combate à criminalidade, nomeadamente à criminalidade organizada.

[27] Acórdão n..º 420/2017, § 13, associado ao processo n..º 917/16, cujo relator é Conselheira Maria de Fátima Mata-Mouros, disponível em TC > Jurisprudência > Acordãos > Acórdão 420/2017. (tribunalconstitucional.pt).

permitir a identificação do utilizador registado, a quem o endereço do protocolo IP estava atribuído, suspeito de autoria de um dos crimes graves referidos*";* em seguida, é também uma medida necessária "na medida em que não é possível configurar um meio menos restritivo para as autoridades competentes procederem à referida identificação*"*.

Por fim, refere o TC que a proporcionalidade, no seu sentido estrito, procura vedar a adoção de medidas que se apresentem como excessivas (desproporcionadas) para atingir os fins visados. Neste juízo é necessário ponderar, de um lado, a natureza relativamente pouco invasiva da privacidade dos dados em questão (dados de base), os quais dizem respeito à identidade do utilizador, e, por outro, o período temporal de conservação (um ano) – após o qual os dados são destruídos (art. 7.º, n.º 1, alínea e), da Lei n.º 32/2008). Esta análise deve depois ser confrontada com a natureza especialmente grave dos crimes em questão e a centralidade destes dados para a condução da investigação criminal.

Aqui, o TC, no Acórdão n.º 268/22, não deteta qualquer irregularidade, tendo optado, fundamentando devidamente a sua posição, por manter a sua jurisprudência anterior. A questão central passa, neste último Acórdão, a ser outra – o da ingerência nos dados de tráfego.

E é aqui que o problema, no entender do TC, reside. Com efeito, este entende que, no caso dos dados de tráfego, gerados a propósito de uma comunicação específica, materializa-se "uma agressão mais intensa à intimidade privada dos sujeitos privados do que a preservação dos dados de base, ao permitirem identificar, a todo o tempo, a posição e os movimentos dos utilizadores"[28].

O TC defende que, ainda que a conservação seja, de facto, adequada e necessária para os fins que pretende proteger, a proporcionalidade só não poderá ser colocada em causa quando exista uma ligação direta entre os dados a conservar (e a agressão do direito fundamental que lhe subjaz) e a perseguição dos objetivos da ação penal. Ora, assim sendo,

[28] Acórdão n..º 268/22, §17.3, a respeito do processo n..º 828/2019, cujo relator é Conselheiro Afonso Patrão, disponível em https://www.tribunalconstitucional.pt/tc/acordaos/20220268.html

a conservação de todos os dados listados no art. 4.º da Lei n.º 32/2008, e de todos os indivíduos, ao ser geral e indiscriminada, é manifestamente desproporcional porque não existe esta relação direta para a conservação.

Assim, o TC entende que esta é uma solução jurídica desequilibrada face às finalidades que pretende alcançar, numa violação direta do art. 18.º, n.º 2 da CRP.

Também o TJUE já tinha entendido que a Diretiva 2006/24 implicava uma restrição desproporcionada aos direitos ao respeito pela vida privada e familiar e à proteção de dados pessoais, consagrados, respetivamente, nos arts. 7.º e 8.º da CDFUE. Em particular, entendia o TJUE que os problemas da Diretiva 2006/24, entre outros, se relacionavam com o facto de esta:

a. Não exigir relação entre os dados conservados e a ameaça à segurança pública, não se limitando a uma conservação em relação (i) a dados relativos a um período de tempo específico e/ou a uma zona geográfica específica e/ou a um círculo de pessoas específicas suscetíveis de estarem envolvidas, de alguma forma, numa criminalidade grave, ou (ii) a pessoas que poderiam contribuir, através da conservação dos seus dados, para a prevenção, deteção ou persecução de infrações graves;
b. Não conter condições substantivas e processuais relativas ao acesso das autoridades nacionais competentes aos dados e à sua subsequente utilização, não estabelecendo que estes têm que estar estritamente limitados ao propósito de prevenir, detetar ou investigar infrações graves (previamente definidas), apenas dispondo que cada Estado-Membro deveria definir os procedimentos a seguir e as condições a cumprir para obter acesso aos dados retidos de acordo com os requisitos de necessidade e proporcionalidade;
c. Exigir que esses dados fossem retidos por um período mínimo de seis meses (sem distinção entre as categorias de dados a

conservar), com base na sua utilidade possível para os fins do objetivo perseguido ou de acordo com as pessoas em questão; ao mesmo tempo, tal período era fixado entre um mínimo de seis meses e um máximo de 24 meses, sem que a determinação do período de conservação fosse baseada em critérios objetivos para garantir esta fosse limitada ao estritamente necessário;

d. Não prever garantias suficientes, no que diz respeito às regras relativas à segurança e proteção dos dados retidos pelos fornecedores de serviços de comunicações eletrónicas, conforme exigido pelo art. 8.º da CDFUE, para assegurar a proteção efetiva dos dados conservados contra o risco de abuso e contra qualquer acesso e utilização ilegal desses dados; em concreto, a diretiva não estabelecia regras específicas e adaptadas (i) à grande quantidade de dados cuja conservação é exigida por essa diretiva, (ii) à natureza sensível desses dados e (iii) ao risco de acesso ilegal a esses dados, regras que serviriam para garantir a integridade e confidencialidade dos dados, sem que sequer tenha sido estabelecida uma obrigação específica aos Estados-Membros para estabelecer tais regras;
e. Não exigir que os dados em questão fossem conservados dentro da União Europeia, não se assegurando a possibilidade de controlo por uma autoridade independente do cumprimento dos requisitos de proteção e segurança, tal explicitamente exigido pelo art. 8.º, n.º 3 da CDFUE, o qual é um componente essencial da proteção das pessoas em relação ao tratamento de dados pessoais[29].

Deste modo, ficou patente que, à luz da CDFUE, é possível a conservação destes dados, desde que exista uma ponderação sobre a

[29] Tribunal de Justiça da União Europeia, Comissão Europeia, apoiada pela Autoridade Europeia para a Proteção de Dados (AEPD), contra República da Áustria, § 37, processo C-614/10, disponível em https://curia.europa.eu/juris/document/document.jsf;jsessionid=E64E601BB3BB3FCFD0DBECA2C34F4641?text=&docid=128563&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=5154569

adequação, face à proteção de um interesse geral relevante. Contudo, e em complemento, ficou também claro que a respetiva regulamentação deve restringir a sua aplicação ao indispensável para aquele objetivo, mediante (i) definição seletiva do universo de dados e de titulares afetados, (ii) o estabelecimento de garantias no acesso das autoridades a essas informações, (iii) a estatuição de critérios objetivos de duração da conservação por atenção aos objetivos visados, e (iv) a criação de mecanismos de segurança de proteção eficazes desses dados contra abusos, utilização e acesso ilícitos.

Como muito bem refere o TC no seu Acórdão, 268/2022, o Acórdão Digital Rights Ireland permitiu delimitar o parâmetro comunitário de admissibilidade das medidas de conservação dos dados de tráfego e de localização. Assim, restavam poucas dúvidas que ponto de partida para um novo regime tinha que ser o Acórdão Digital Rights Ireland, e que todas as críticas e falhas ao regime por este feitas deveriam ser resolvidas num novo regime congruente com estas críticas.

4. O REGIME ATUAL DOS METADADOS

Após uma extensa e duradoura discussão sobre o tema[30], bem como várias tentativas, a Assembleia da República conseguiu finalmente aprovar alterações à Lei n.º 32/2008, com a publicação da Lei n.º 18/2024, de 5 de fevereiro

A nova versão do diploma determina que os dados de tráfego e de localização apenas podem ser objeto de conservação para fins de investigação, deteção e repressão de crimes graves por parte das autoridades competentes, mediante autorização judicial, de caráter urgente e decidido no período máximo de 72h.

[30] Que envolveu uma nova proposta da Assembleia da República que lhe foi devolvida, perante a submissão, pelo Presidente, à fiscalização preventiva do TC, uma vez que a proposta não resolvia a questão da conservação geral e indiscriminada dos dados de tráfego.

A este respeito, surgem dúvidas sobre a efetiva utilidade deste método. Com efeito, uma das maiores críticas feitas a este procedimento – também designado por *quickfreeze*[31]- é relativamente à sua adequação, face à finalidade prosseguida com esta conservação, pelo simples facto de que, com frequência, não se demonstra totalmente eficaz tendo em vista a sua finalidade (sobretudo, e naturalmente, quando comparada com conservação generalizada), motivo pelo qual muitas vezes este método fica excluído enquanto solução única e isolada. A nível europeu, este método não é totalmente compatível com a jurisprudência do TJUE[32], que exige que a conservação desses dados seja limitada ao estritamente necessário e que esteja sujeita a garantias efetivas e a um controlo independente.

De resto, esta nova versão do diploma apenas altera o período de conservação dos dados de tráfego e localização (cujo exato período de conservação deve ser determinado na autorização judicial), mantendo o prazo de conservação de um ano, a contar da conclusão da comunicação, para os dados de base, assim como os endereços de IP.

Este regime merece, naturalmente, algumas críticas, como as que se exporão em seguida, bem como uma breve análise sobre a sua conjugação com o disposto na Lei n.º 41/2004.

A Lei n.º 41/2004 prevê que, pelo menos alguns dos dados de tráfego (desde que anonimizados) possam ser conservados pelas operadoras para efeitos de execução dos próprios contratos. Contrariamente ao que ocorria com a Lei n.º 32/2008, esta disposição estipula uma faculdade, e não uma obrigação, de os operadores conservarem tais dados.

---

[31] Que se traduz numa conservação para o futuro, desde o pedido do Ministério Público, válida apenas para o caso concreto, só podendo ser ordenada tendo como fundamento concreto a verificação de uma determinada suspeita. Em Portugal, é exemplo da utilização deste método o art. 12..º da Lei do Cibercrime.

[32] Por exemplo, Veja-se, por exemplo, o acórdão do Tribunal de Justiça da União Europeia, Tele2 Sverige AB contra Post och telestyrelsen, datado de 21 de dezembro de 2016, processo C203/15, disponível em https://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=5157465.

Neste sentido, a Lei n.º 41/2004 prevê que os dados de tráfego necessários à faturação dos assinantes e ao pagamento de interligações só podem ser tratados até ao final do período durante a qual a fatura pode ser legalmente contestada ou o pagamento reclamado (que, de acordo com a Lei n.º 23/96 de 26 de julho – aplicável *ex vi* art. 6.º, n.º 3 da Lei n.º 41/2004 – é de seis meses). Tal significa que as operadoras podem conservar os dados de tráfego para efeitos de faturação e proteção comercial durante seis meses.

Não é, contudo, evidente, se a listagem de dados de tráfego que podem ser conservados ao abrigo da Lei n.º 41/2004 se justaponha totalmente ao catálogo de dados existente na Lei n.º 32/2008, sobretudo porque o grau de granularidade com que se lista os dados de tráfego a conservar é bastante distinta – ou seja, uma das listagens é muitíssimo mais concreta que a outra.

No limite, mesmo dentro da mesma categoria de dados de tráfego não é de excluir a possibilidade de se ter certos tipos de dados de tráfego que só podem ser conservados mediante a referida autorização judicial e outros tipos de dados de tráfego que podem ser conservados sem que tal seja necessário, desde que por associação à execução do contrato com o titular dos dados.

Também não é evidente se, guardando as operadoras todos os dados que legalmente *podem* guardar, com base na necessidade de faturação, se o Ministério Público se encontra legitimado, se assim entender, a requerer também esses dados.

Sem prejuízo do facto de quaisquer tratamentos efetuados pelas autoridades competentes, no âmbito da prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública, se encontrarem excluídos do âmbito de aplicação material do Regulamento Geral sobre a Proteção de Dados ("RGPD"), tal como descrito no seu artigo 2.º, n.º 2, alínea d), qualquer tratamento de dados efetuado pelos prestadores de serviços de comunicações eletrónicas encontra-se, de todo o modo, sujeito ao RGPD.

Este diploma obriga a que os dados sejam tratados com um determinado fundamento de licitude que, por sua vez, se encontra ancorado na finalidade que justifica tal tratamento, não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades (cfr. arts. 5.º, n.º 1, alínea b) e arts. 6.º).

Um dos fundamentos de licitude para o tratamento de dados pessoais, previstos pelo RGPD, no seu art. 6.º, é a obrigação legal. Com a Lei n.º 38/2008, existia uma obrigação legal de os operadores conservarem todos os metadados ali listados, durante o período de um ano, para finalidades de repressão de criminalidade grave, e, portanto, não se suscitavam dúvidas quanto à conformidade deste tratamento com o RGPD. Quando estes dados eram requeridos pelo Ministério Público, eram simplesmente entregues, sem que quaisquer questões se colocassem a este respeito.

Ora, atualmente, e com esta alteração de regime, esta obrigação legal de conservação inexiste relativamente a alguns dos dados de tráfego, ainda que continue a existir claramente relativamente a respeito dos dados de base.

Só que, para finalidades de execução do contrato e faturação, ao abrigo da Lei n.º 41/2004, os operadores podem continuar a conservar, pelo menos, muitos dos dados que eram conservados ao abrigo da Lei n.º 38/2008.

Quid iuris se o Ministério público solicita estes dados aos operadores? Por um lado, os dados não podem, ao abrigo do RGPD, ser tratados para outras finalidades que não aquelas para as quais são recolhidos, sem prejuízo de um eventual teste de compatibilidade; por outro, existe um dever de colaboração com as autoridades judiciárias, pelo que será difícil os operadores obviarem-se ao cumprimento desta obrigação, até porque este pedido poderá constituir, ele próprio, fundamento de licitude para o tratamento, enquanto obrigação legal.

A este respeito, e sendo difícil argumentar que os operadores se podem recusar a cumprir com tais pedidos, será também complicado não argumentar que não nos encontramos perante uma *porta lateral*

para a obtenção dos metadados, quando existe expressamente um regime muito particular a obedecer nesta matéria[33].

No demais, e por fim, de referir que não restam dúvidas que a Assembleia da República foi obrigada a tomar a decisão para assegurar que o crivo de constitucionalidade era ultrapassado e, nessa medida, foi bem-sucedida. Impõem-se, contudo, uma discussão importante sobre a ponderação e juízo de proporcionalidade feitos pelo TC.

Efetivamente, resulta das decisões aqui descritas do TC que os dois tipos de tratamentos de metadados – i.e. a conservação e o acesso – foram analisados de forma praticamente conjunta.

De referir, ainda assim, que o TC dedica parte do Acórdão n.º 268/2022 a justificar esta análise conjunta. Com efeito, apesar de admitir que a compressão nos direitos fundamentais não ocorre toda por igual nem no mesmo momento, o TC refere que "apesar de a sua simples conservação constituir, por si só, uma limitação daqueles direitos, a intensidade da restrição depende em boa medida das garantias inerentes à transmissão e acesso a esses dados"[34]. É certo que esta já havia sido a posição tomada pelo Acórdão n.º 420/2017, mas também será injusto dizer, como referiu o TC, que não se identificam motivos para alterar esta abordagem.

A Provedora de Justiça, quando apresentou o pedido de apreciação ao TC, havia argumentado em sentido diverso e a sua argumentação justifica, no mínimo, uma ponderação redobrada a este respeito. No seu entender, "perante a existência de dois momentos autónomos de

---

[33] Ver a este respeito o Acórdão da Tribunal da Relação do Porto, de 7 de dezembro de 2022, cujo n..º do processo é 5011/22.2JAPRT-A.P1, e o relator Pedro Vaz Pato, disponível em Acórdão do Tribunal da Relação do Porto (dgsi.pt), no qual o Tribunal esclarece que "tendo o acórdão do Tribunal Constitucional declarado a inconstitucionalidade, com força obrigatória geral, dos arts. 4..º, 6..º e 9..º da Lei n..º 32/2008, de 17 de julho (Lei relativa à conservação de dados gerados ou tratados no contexto de oferta de serviços de comunicações eletrónicas), não podemos tentar tornear esse acórdão, *deixando entrar pela janela* aquilo a que ele *fechou a porta*; ou seja, não podemos recorrer a outras normas para obter o mesmo efeito que resultaria da aplicação das normas declaradas inconstitucionais sem que essas outras normas contenham aquelas garantias que faltam a estas e que levaram a essa declaração de inconstitucionalidade."

[34] Acórdão n..º 286/22, § 14, a respeito do processo n..º 828/2019, cujo relator é Conselheiro Afonso Patrão, disponível em https://www.tribunalconstitucional.pt/tc/acordaos/20220268.html

agressão aos direitos, não é de todo legítimo confundi-los de acordo com uma *lógica de compensação".*

Assim, entendia a Provedora de Justiça que uma dogmática correta de direitos fundamentais exigiria que o TC analisasse*, "*autonomamente, a conformidade constitucional de cada uma das agressões aos direitos, em nada podendo o regime de acesso e de utilização dos dados interferir na análise da conformidade constitucional, designadamente e no que respeita as exigências decorrentes do princípio da proporcionalidade, da agressão aos direitos implicada na própria imposição legal de conservação de dados*".*

Acresce que, além de se tratar de dois momentos de agressão diferentes, a intensidade da sua agressão não é comparável. É inegável que, ainda que exista necessariamente uma compressão do direito fundamental à privacidade com a conservação dos dados, a gravidade da mesma não é, nem pode ser, comparável à compressão que existe no caso do acesso desses mesmos dados. Por outras palavras: se os dados forem conservados, é inegável que há um perigo de acesso indevido que lhes subjaz, do qual é difícil de fugir; contudo, também não é possível ignorar que é o próprio acesso em si que comprime em larga medida o direito à privacidade, porque, no limite, se ninguém aceder a tais dados, não há como o direito à privacidade ser violado.

O problema da análise conjunta é o perigo da atribuição de uma gravidade inconsistente com a compressão que a conservação efetivamente representa e confundir a agressão perpetuada pelo acesso com a da conservação. Ao analisar-se a conservação à luz dos perigos do acesso, a análise da proporcionalidade, na ponderação de valores na balança ficará, inevitavelmente, distorcida, pelo simples facto de que se está a atribuir uma intensidade de agressão à conservação que não lhe pertence.

Ademais, sendo os perigos do acesso manifestamente mais significativos do que o da mera conservação, mas atribuindo os primeiros à segunda, a tendência vai ser obviamente de considerar que esta é

injustificável, o que, por sua vez, poderá levar-nos a concluir que a conservação não é legítima quando, na verdade, até pode ser.

O próprio acórdão Digital Rights Irelands sublinha, precisamente, que o conteúdo essencial do direito fundamental não é afetado em face das medidas de proteção que são implementadas. Efetivamente, refere o TJUE que "conservação dos dados também não é suscetível de afetar o conteúdo essencial do direito fundamental à proteção dos dados pessoais, consagrado no artigo 8.º da CDFUE, uma vez que a Diretiva 2006/24 prevê, no seu artigo 7.º, uma regra relativa à proteção e à segurança dos dados, o que obriga a que sejam respeitados certos princípios de proteção e de segurança dos dados pelos fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, princípios de acordo com os quais os EstadosMembros devem assegurar a adoção de medidas técnicas e organizacionais adequadas contra a destruição acidental ou ilícita, a perda ou a alteração acidental dos dados"[35].

Não foi, contudo, este o entender do TC. De resto, e pelo menos para já, a questão parece ter ficado disciplinada com este novo regime.

5. CONCLUSÕES

O presente artigo visava, por um lado, oferecer um enquadramento simples – dentro daquilo que são os limites de um tema, por natureza, complexo – sobre a temática dos metadados. Em particular, procurou-se refletir sobre as preocupações e discussões que têm tido lugar nos últimos anos a este respeito, nomeadamente nos Acórdãos do TC e do TJUE. Por outro lado, discutiu-se, de forma

[35] Tribunal de Justiça da União Europeia, Digital Rights Ireland Ltd contra Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Irlanda, §40, datado de 8 de abril de 2014, processos apensos C293/12 e C594/12, disponível em https://curia.europa.eu/juris/document/document.jsf;jsessionid=3CE25888D6478AA3CC9ED7B78735A64F?text=&docid=150642&pageIndex=0&doclang=pt&mode=req&dir=&occ=first&part=1&cid=2712231

muito breve, o regime atual – também dentro dos limites do que é possível analisar nesta fase a este respeito, em que a realidade prática não é, ainda, possível de conhecer na sua totalidade.

Conforme descrito ao longo deste artigo, a discussão em torno dos metadados no contexto das comunicações eletrónicas, bem como da definição dos limites e das garantias da conservação e do acesso a esses dados tem sido particularmente longa e controversa, quer a nível europeu, quer a nível nacional.

Considerando a evolução legislativa e jurisprudencial em ambas as vertentes, antevê-se que a evolução dinâmica que se assistiu nos últimos anos relativamente ao enquadramento jurídico dos metadados ainda se mantenha futuramente, exigindo, para já, uma constante ponderação entre os diferentes valores e interesses envolvidos, nomeadamente ao nível dos tribunais, e uma adaptação com o peso e medida das novas realidades tecnológicas e sociais que vão tendo lugar.

No que respeita, em específico, ao novo regime aprovado relativamente aos metadados, através Lei n.º 18/2024, de 5 de fevereiro, e embora este seja, como ficou patente, merecedor de críticas, parece resolver, no imediato, as questões apontadas pelo TC. Sem prejuízo, só a sua aplicação prática dirá se as questões relativas a esta temática ficaram, de forma definitiva, resolvidas.