Análise das decisões do Tribunal Constitucional no que toca à matéria dos Metadados*

Ana Raquel Conceição
Professora Convidada (equiparada a auxiliar) da Escola de Direito da Universidade do Minho

Resumo: O presente trabalho assenta na análise das decisões do Tribunal Constitucional no que concerne à temática dos *Metadados*.

Analisamos, sumariamente, o conceito de *Metadados* e a sua relevância probatória.

Fazemos uma incursão sobre a argumentação constante dos Acórdãos do Tribunal Constitucional n.os 268/2022 e 800/2023, dando nota, tal como consta da referida jurisprudência, do Acórdão do TJUE denominado *Digital Rights Ireland*, que imprimiu um novo sentido de decisão e interpretação da nossa Lei n.º 32/2008, de 17/7, conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas, tendo por referência arts. 7.º e 8.º da CDFUE, bem como o juízo contido no Acórdão *SpaceNet*, onde se reafirma o juízo decisório.

Com a presente análise afere-se e reafirma-se que a descoberta da verdade material segue o caminho de respeito pelos direitos, liberdade e garantias. Mesmo que tal mensagem possa não ser bem interpretada, na atualidade, consideramos que essa é, e deverá sempre ser, a bússola do respeito pela dignidade da condição da pessoa humana.

Palavras-chave: Metadados / Tribunal Constitucional / Privacidade / Direitos humanos

Abstract: This work is based on the analysis of the decisions of the Portuguese Constitutional Court regarding the topic of *Metadata*.

---

* O presente texto resulta, no essencial, da comunicação apresentada na aula aberta "Os Metadados na investigação da Lei n.º 18/2024", Escola Superior de Tecnologia e Gestão, que ocorreu no dia 3/4/2024, Felgueiras, podendo, por este facto, constar no texto alguma linguagem usual na oralidade da exposição.

We will, briefly, analyze the concept of *Metadata* and its relevance, through an incursion into the arguments contained in the decisions 268/2022 and 800/2023 of the Portuguese Constitutional Court, taking note, as stated in the aforementioned case law, of the CJEU ruling called *Digital Rights Ireland*, which gave a new meaning to the decision and interpretation of our law n.º 32/2008, of 17/7, conservation of data generated or processed in the context of offering electronic communications services, with reference to articles 7th and 8th of the CDFUE, as well as the judgment contained in the *SpaceNet* decision, where the decision-making judgment is reaffirmed.

With this analysis, it's verified that the discovery of procedural truth, follows the path of respect for rights, freedoms and guarantees. Even though such a message may not be well interpreted, today, we consider that this is, and always should be, the compass of respect for the dignity of the human condition.

Keywords: *Metadata* / Portuguese Constitucional Court / Privacy / Human Rights

Breves noções introdutórias

A teoria da prova é o verdadeiro cerne do processo penal. O regime jurídico da prova reflete os *achaques e a lisura das civilizações*[1]. A previsão das suas regras e limites é o instrumento que permite o funcionamento de um processo penal orientado para a descoberta da verdade material, mas respeitador dos direitos fundamentais dos indivíduos.

Hoje, mais do que nunca, existe uma grande preocupação no que concerne ao regime legal da prova em processo penal. As novas formas de criminalidade que hoje nos invadem, oriundas de uma sociedade globalizada e em rede, obrigam a que dotemos o processo penal de novas formas de investigação criminal. Inovação que provocará a utilização de novos meios de prova e de obtenção de prova ou o reforço de certos meios de obtenção de prova mais eficazes na descoberta da verdade material. Eficácia que, muitas vezes, não é sinónimo de respeito pelos direitos fundamentais do indivíduo.

[1] Susana Aires de Sousa, "Agent provocateur e meios enganosos de prova. Algumas reflexões", *in* Liber Discipulorum *para Jorge de Figueiredo Dias*, Coimbra Editora, 2003, p. 1208.

A atual situação socioeconómica; a alteração cultural de paradigma resultante dos extraordinários avanços tecnológicos, incluindo, entre outros, ferramentas baseadas em inteligência artificial (IA) e tecnologias; o crescente volume e variedade de dados disponíveis, bem como a velocidade de troca de dados; a interconectividade entre dispositivos e a fusão dos mundos físico, digital e biológico, combinado com a velocidade das novidades tecnológicas e da amplitude e profundidade com que estão a afetar diferentes setores das nossas vidas – não apenas a maneira como trabalhamos, nos comunicamos e nos relacionamos, mas também cuidados de saúde, ambiente e alterações climáticas, segurança, economia e padrões de consumo, política e processos de produção –, são os sinais de que estamos perante uma "Sociedade Global", que é caracterizada pela "*interligação mundial de computadores, redes e sistemas informáticos e telemáticos*"[2].

A adaptação referida é necessária; porém, para ser legítima, tem sempre de operar com o respeito pelas bases do Estado de Direito democrático, em especial a dignidade da pessoa humana. A proteção dos direitos fundamentais é algo que tem de estar sempre presente no processo penal, principalmente no âmbito do regime jurídico da prova. É esta proteção o mais importante princípio de legitimação das proibições de prova.

Tal como refere FIGUEIREDO DIAS, a legalidade dos meios de prova, bem como as regras gerais de produção da prova e as chamadas proibições de prova são condições de validade processual da prova, por isso mesmo, *critérios da própria verdade material*[3]. Assim, serão inadmissíveis, de uma forma geral, os meios de prova que corporizem um ilícito material substantivo, pois, se se pudessem valorar, no processo penal, meios de prova obtidos com a lesão ou o perigo de lesão de um bem jurídico penalmente protegido, o Estado estaria a provar a prática de um crime utilizando como meio dessa mesma prova um outro crime.

Não perdendo o foco, vamos, desta feita, analisar a jurisprudência do Tribunal Constitucional relativa à tão discutida temática dos Metadados.

---

[2] VERA MARQUES DIAS, "A problemática da Investigação do Cibercrime", in *Datavenia. Revista jurídica digital*, Ano 1, n.º 1, julho-dezembro, 2012, p. 64.

[3] JORGE DE FIGUEIREDO DIAS, *Direito processual penal* (lições coligidas por Maria João Antunes), Secção de Textos da Faculdade de Direito da Universidade de Coimbra, 1988-1989, p. 133 (itálico nosso).

1. O Acórdão n.º 268/2022[4]:

O Acórdão n.º 268/2022 teve origem num pedido de fiscalização da constitucionalidade, de requerimento da Provedora da Justiça, cujo objeto foi a apreciação e a declaração, com força obrigatória geral, da inconstitucionalidade, das normas contidas nos arts. 4.º, 6.º e 9.º da Lei dos Metadados (Lei n.º 32/2008, de 17/7, conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas). Analisemos, sumariamente, qual o teor de tais normativos.

O art. 4.º diz respeito à categoria de dados a conservar[5]; o art. 6.º é referente ao período de conservação[6]; o art. 9.º trata, por sua vez, da transmissão de dados[7].

---

[4] Disponível em *https://www.tribunalconstitucional.pt/tc/acordaos/20220268.html*.

[5] Esta era a sua versão original:

"1 – Os fornecedores de serviços de comunicações electrónicas publicamente disponíveis ou de uma rede pública de comunicações devem conservar as seguintes categorias de dados:

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.

2 – Para os efeitos do disposto na alínea *a)* do número anterior, os dados necessários para encontrar e identificar a fonte de uma comunicação são os seguintes:

a) 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;

b) No que diz respeito ao acesso à Internet, ao correio electrónico através da Internet e às comunicações telefónicas através da Internet:

i) Os códigos de identificação atribuídos 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.

3 – Para os efeitos do disposto na alínea *b)* do n.º 1, os dados necessários para encontrar e identificar o destino de uma comunicação são os seguintes:

a) No que diz respeito às comunicações telefónicas nas redes fixa e móvel:

i) Os números marcados 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;

Face aos dois primeiros artigos, estava em causa a verificação dos requisitos para a legitimidade constitucional da restrição dos direitos fundamentais, como o direito à reserva da vida privada, o direito ao livre desenvolvimento da pessoa e o direito à proteção de dados.

---

b) No que diz respeito ao correio electrónico através da Internet e às comunicações telefónicas através da Internet:

i) O código de identificação do utilizador ou o número de telefone do destinatário pretendido, ou de uma comunicação telefónica através da Internet;

ii) Os nomes e os endereços dos subscritores, ou dos utilizadores registados, e o código de identificação de utilizador do destinatário pretendido da comunicação.

4 – Para os efeitos do disposto na alínea *c)* do n.º 1, os dados necessários para identificar a data, a hora e a duração de uma comunicação são os seguintes:

a) No que diz respeito às comunicações telefónicas nas redes fixa e móvel, a data e a hora do início e do fim da comunicação;

b) No que diz respeito ao acesso à Internet, ao correio electrónico 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 electrónico através da Internet ou de comunicações através da Internet, com base em determinado fuso horário.

5 – Para os efeitos do disposto na alínea *d)* do n.º 1, os dados necessários para identificar o tipo de comunicação são os seguintes:

a) No que diz respeito às comunicações telefónicas nas redes fixa e móvel, o serviço telefónico utilizado;

b) No que diz respeito ao correio electrónico através da Internet e às comunicações telefónicas através da Internet, o serviço de Internet utilizado.

6 – Para os efeitos do disposto na alínea *e)* do n.º 1, os dados necessários para identificar o equipamento de telecomunicações dos utilizadores, ou o que se considera ser o seu equipamento, são os seguintes:

a) No que diz respeito às comunicações telefónicas na rede fixa, os números de telefone de origem e de destino;

b) 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 activação inicial do serviço e o identificador da célula a partir da qual o serviço foi activado;

Neste sentido, o Tribunal Constitucional entendeu que o legislador português não determinou que o armazenamento dos dados, de tráfego e localização, ocorresse em território europeu, o que colocou em colisão com o art. 35.º, n.os 1 e 4, da Constituição da República Portuguesa (CRP), que consagra o direito à proteção de dados pessoais. Ora, ocorrendo o armazenamento fora da União Europeia, isso põe em causa "*a efetividade do exercício dos direitos de informação e de acesso, entre outros, dos titulares dos estados*". Em virtude disto, considerou que os arts. 4.º e 6.º estavam feridos

---

c) No que diz respeito ao acesso à Internet, ao correio electrónico 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.

7 – Para os efeitos do disposto na alínea *f)* do n.º 1, os dados necessários para identificar a localização do equipamento de comunicação móvel são os seguintes:

a) O identificador da célula no início da comunicação;

b) Os dados que identifiquem a situação geográfica das células, tomando como referência os respectivos identificadores de célula durante o período em que se procede à conservação de dados.".

[6] Esta era a sua versão original:

"As entidades referidas no n.º 1 do artigo 4.º devem conservar os dados previstos no mesmo artigo pelo período de um ano a contar da data da conclusão da comunicação.".

[7] Esta era a sua versão original:

"1 – A transmissão dos dados referentes às categorias previstas no artigo 4.º 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, detecção e repressão de crimes graves.

2 – A autorização prevista no número anterior só pode ser requerida pelo Ministério Público ou pela autoridade de polícia criminal competente.

3 – Só pode ser autorizada a transmissão de dados relativos:

a) Ao suspeito ou arguido;

b) A pessoa 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

c) A vítima de crime, mediante o respectivo consentimento, efectivo ou presumido.

4 – A decisão judicial de transmitir os dados deve respeitar os princípios da adequação, necessidade e proporcionalidade, designadamente no que se refere à definição das categorias de dados a transmitir e das autoridades competentes com acesso aos dados e à protecção do segredo profissional, nos termos legalmente previstos.

5 – O disposto nos números anteriores não prejudica a obtenção de dados sobre a localização celular necessários para afastar perigo para a vida ou de ofensa à integridade física grave, nos termos do artigo 252.º-A do Código de Processo Penal.

6 – As entidades referidas no n.º 1 do artigo 4.º devem elaborar registos da extracção dos dados transmitidos às autoridades competentes e enviá-los trimestralmente à CNPD.".

de inconstitucionalidade, por violarem o art. 35.º, n.os 1 e 4, da CRP à luz dos arts. 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia (CDFUE ou Carta).

Também entendeu que a conservação generalizada e indiscriminada desses mesmos dados ia para além dos limites impostos pelo princípio da proporcionalidade, considerando assim inconstitucional, mais uma vez, os artigos suprarreferidos por violação dos arts. 35.º, n.os 1 e n.º 4, e 26.º, n.º 1, conciliados com o art. 18.º, todos da CRP.

No que respeita ao art. 9.º da Lei dos Metadados, o Tribunal Constitucional chamou a atenção para a ausência de notificação ao titular dos dados da eventualidade de acesso aos mesmos, sendo que tal ausência restringe o direito à proteção dos dados pessoais, como também à tutela jurisdicional efetiva, prevista no art. 20.º da CRP, pois o desconhecimento pelo titular implica que nunca pode reagir a tal restrição e pode estar sujeito a acessos abusivos e ilícitos, sem possibilidade de atuar em conformidade. E, por essa razão, o Tribunal considerou igualmente inconstitucional o art. 9.º da Lei n.º 32/2008, uma vez que este artigo não prevê em qualquer circunstância uma notificação ao visado, violando os arts. 35.º, n.º 1, 20.º, n.º 1, e 18.º da CRP.

Note-se que a maioria decisória que determinou a inconstitucionalidade dos referidos artigos da apelidada Lei dos Metadados foi influenciada pelo juízo de proporcionalidade realizado por acórdão do Tribunal de Justiça da União Europeia (TJUE).

Na verdade, o TJUE declarou a invalidade da Diretiva 2006/24/CE (Acórdão de 8/4/2014, *Digital Rights Ireland*, procs. apensos C-293/12 e C-594/12) – que harmonizava as medidas de conservação de dados relativos a comunicações e sua transmissão às autoridades com competência criminal –, mas nem por isso se excluíram tais medidas do âmbito de aplicação do direito europeu. Simplesmente, não mais os Estados-Membros se encontram obrigados a adotar as providências que aquela impunha; embora as medidas nacionais que permitam ou visem uma intromissão nas comunicações eletrónicas fiquem sujeitas às obrigações decorrentes do disposto no art. 15.º da Diretiva 2002/58/CE, só sendo conformes ao direito europeu quando, nos termos deste artigo, "constituam uma medida necessária, adequada e proporcionada numa sociedade democrática para salvaguardar a segurança nacional (ou seja, a segurança do Estado), a defesa, a segurança pública, e a prevenção, a investigação, a deteção e a repressão de infrações penais ou a utilização não autorizada do sistema de comunicações eletrónicas"[8].

[8] Disponível em *eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:62012CJ0293*.

O TJUE concluiu pela invalidade das normas da Diretiva de 2006, por implicarem uma restrição desproporcionada dos 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, e por estabelecerem de forma indeterminada o leque de crimes cuja investigação ou repressão pode admitir o acesso aos dados conservados (Acórdão *Digital Rights Ireland*, *cit.*, n.os 26 a 29; e 41 a 43). Sendo o direito derivado da União Europeia parametrizado pelo respetivo direito primário – e assumindo a CDFUE justamente esse valor (cfr. n.º 1 do art. 6.º do Tratado da União Europeia) –, concluiu o Juiz europeu não estarem preenchidos os pressupostos da sua restrição (n.º 1 do art. 52.º da CDFUE).

O Acórdão *Digital Rights Ireland* permite, assim, delimitar o parâmetro europeu de admissibilidade das medidas de conservação dos dados de tráfego e de localização: à luz da Carta, é possível a sua estatuição (sendo adequadas à proteção de um interesse geral relevante), embora a regulamentação deva restringir a sua aplicação ao indispensável para aquele objetivo, mediante: *i)* definição seletiva do universo de dados e de titulares afetados; *ii)* estabelecimento de garantias no acesso das autoridades a essas informações; *iii)* estatuição de critérios objetivos de duração da conservação por atenção aos objetivos visados; *iv)* criação de mecanismos de segurança de proteção eficaz desses dados contra abusos, utilização e acesso ilícitos[9].

O TJUE considerou que a conservação só era admissível quando obedeça a certos critérios: um período temporal, uma zona geográfica determinada e um círculo de pessoas determinado. Porém, tais critérios não são tolerados, no entender do Tribunal Constitucional, pela norma do art. 35.º, n.º 3, da CRP, que permite apenas que o legislador autorize tratamento informático de dados relativos à vida privada "com garantias de não discriminação"[10]. Assim, considera o entendimento do TJUE incorreto, sendo que a norma que delimita o âmbito subjetivo da conservação de dados viola o princípio da igualdade e proibição da discriminação.

É de salientar o voto de vencido lavrado no acórdão do Tribunal Constitucional, da autoria do Juiz Conselheiro Lino José Ribeiro, revelador da não unanimidade da votação, o qual realça a existência de um conflito de dois valores, pela existência de um período de conservação de dados: o da liberdade e segurança,

[9] Acórdão *Digital Rights Ireland*, *cit.*, n.os 51 e 56 a 59.
[10] *Idem*.

previsto no art. 27.º da CRP, e o da privacidade e autodeterminação dos dados pessoais, consagrado nos arts. 26.º e 35.º da CRP. No entanto, considera que os bens ou valores em causa não têm uma ponderação tão proeminente, que justifique o sacrifício do valor da segurança, como acabou por resultar da declaração de inconstitucionalidade que a maioria defendeu. Entende ainda o referido Juiz Conselheiro que a Lei n.º 32/2008, na concordância prática entre os valores em causa, conseguiu um equilíbrio que satisfaz razoavelmente ambos os direitos. Realça o facto de que, com a declaração da inconstitucionalidade, os fornecedores de serviços apenas podem conservar os dados quando a autoridade competente os solicitar durante uma investigação criminal, situação a que corresponde a preservação expedita de dados, que não se mostra eficaz para garantir a recolha da prova digital em processo penal. Dadas as circunstâncias em que os dados são retidos, considera não ser excessiva a restrição ao direito à autodeterminação informativa, consagrado no art. 35.º da CRP. Entende, na verdade, que as normas deste mesmo artigo permitem ao legislador definir as "*condições em que os dados pessoais podem ser automatizados (n.º 2), a autorizar o tratamento de dados referentes à vida privada (n.º 3) e a especificar as situações excecionais em que terceiros podem ter acesso aos dados (n.º 4).*"[11].

Assim, com esta decisão judicial, a conservação e o acesso aos dados de tráfego e de localização e a sua utilização probatória deixaram de encontrar fundamento na Lei n.º 32/2008, de 17/7. É este o teor do dispositivo desta decisão:

"a) *Declarar a inconstitucionalidade, com força obrigatória geral, da norma constante do artigo 4.º da Lei n.º 32/2008, de 17 de julho, conjugada com o artigo 6.º da mesma lei, por violação do disposto nos números 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 n.º 18.º, todos da Constituição;*

b) *Declarar a inconstitucionalidade, com força obrigatória geral, da norma do artigo 9.º da Lei n.º 32/2008, de 17 de julho, relativa à transmissão de dados armazenados às autoridades competentes para investigação, deteção e repressão de crimes graves, na parte em que não prevê uma notificação ao visado de que os dados conservados foram acedidos pelas autoridades de investigação criminal, a partir do momento em que tal comunicação não seja suscetível de comprometer as investigações nem a vida ou integridade física de terceiros, por violação do disposto no 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 Constituição.*"

[11] Disponível em *https://www.tribunalconstitucional.pt/tc/acordaos/20220268.html*.

De modo a afastar o suprarreferido juízo de constitucionalidade, a Lei n.º 32/2008 foi alterada pela Lei n.º 79/2021, de 24/11. O legislador vem, agora, e nas suas próprias palavras, *declaradamente conformar o regime em causa com as conclusões do acórdão do Tribunal Constitucional*[12].

Todavia, o Presidente da República, de modo a assegurar a certeza e a segurança jurídicas, face a esta temática tão sensível e tão mediatizada, voltou a pedir ao Tribunal Constitucional que aferisse se tal propósito do legislador havia sido atingido. Importava, pois, verificar se o Tribunal considera que a Assembleia da República teve sucesso nesta sua deliberação, surgindo assim o segundo acórdão do Tribunal Constitucional sobre esta temática.

2. O Acórdão n.º 800/2023[13]:

O Presidente da República enviou ao Tribunal Constitucional a apreciação da nova redação dos artigos cujo teor havia sido declarado inconstitucional. Em suma, com o seguinte pedido:

– a norma constante do art. 2.º, na parte em que altera o art. 4.º da Lei n.º 32/2008;

– a norma constante do art. 2.º, na parte em que altera o art. 4.º quando conjugado com o art. 6.º da Lei n.º 32/2008;

– a norma constante do art. 2.º, na parte em que altera o art. 9.º da Lei n.º 32/2008.

Resulta da leitura das normas sindicadas que, não obstante ter sido reduzido o prazo para a conservação dos dados de tráfego, pode interpretar-se que se pode continuar a permitir a sua recolha indiscriminada, o que pode não se conformar com o decidido pelo Tribunal no acórdão citado. O Tribunal afirmou então que a recolha indiscriminada destes dados violaria, só por si, o princípio da proporcionalidade, perdendo relevância a apreciação dos demais elementos, entre os quais o prazo.

De igual modo, importa verificar se a notificação ao visado, nos termos em que é prevista na nova redação do artigo 9.º, satisfaz as exigências constantes do referido acórdão do Tribunal Constitucional, designadamente no que respeita ao princípio da proporcionalidade[14].

---

[12] Disponível em *https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?artigo_id=3476A0001&nid=3476&tabela=leis&pagina=1&ficha=1&so_miolo=&nversao=*.

[13] Disponível em *https://www.tribunalconstitucional.pt/tc/acordaos/20230800.html*.

[14] *Ibidem*.

Mais uma vez, antes de tomar posição, o Tribunal Constitucional afere da jurisprudência dos Tribunais europeus, dando nota de que cinco meses apenas após a prolação do Acórdão n.º 268/2022 foi exarado, pela Grande Secção do Tribunal de Justiça, em 20/9/2022, o Acórdão *SpaceNet e Telekom Deutschland*[15] (doravante, Acórdão *SpaceNet*), resultante de dois processos apensos, da República Federal da Alemanha contra *SpaceNet AG* (proc. C-793/19) e contra *Telekom Deutschland GmbH* (proc. C-794/19) – o qual se apoia, em larga medida, em diversos arestos citados no Acórdão do Tribunal Constitucional e, sobretudo, no Acórdão *Commissioner of An Garda Síochána*[16], de 5/4/2022 (proc. C-140/20), prolatado 14 dias antes do Acórdão n.º 268/2022.

O juízo contido no Acórdão *SpaceNet* e a fundamentação respetiva não trazem novidades significativas à jurisprudência do TJUE, tal como extensamente examinada no Acórdão n.º 268/2022, reafirmando as suas linhas fundamentais. O confronto do dispositivo do Acórdão do Tribunal Constitucional ora sob o escrutínio com o Acórdão *La Quadrature du Net*, examinado no Acórdão deste Tribunal de 2022, permite confirmar a essencial proximidade entre eles, assinalando essa linha de continuidade na jurisprudência do Tribunal de Justiça que é aqui pressuposta.

Assim, salientaram-se como sendo as suas principais matrizes, no sentido da jurisprudência anterior convocada no Acórdão n.º 268/2022, as seguintes:

i. o papel do princípio da confidencialidade tanto das comunicações eletrónicas como dos respetivos dados de tráfego;

ii. o facto de o legislador da União ter pretendido "assegurar a continuação de um elevado nível de proteção dos dados pessoais e da privacidade no que diz respeito a todos os serviços de comunicações eletrónicas";

iii. a necessidade de proteger os utilizadores dos serviços de comunicações eletrónicas contra os riscos para os seus dados pessoais e a sua vida privada, resultantes das novas tecnologias, em particular o pleno respeito pelos direitos consignados nos arts. 7.º e 8.º da Carta, relativos, respetivamente, à proteção da vida privada e à proteção dos dados pessoais;

iv. o facto de a conservação de dados de tráfego e de dados de localização constituir, em si mesma, uma derrogação da proibição, prevista no art. 5.º, n.º 1,

[15] Disponível em *https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:62019CJ0793*.

[16] Disponível em *https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:62017CJ0378*.

da Diretiva 2002/58/CE, imposta a qualquer pessoa distinta dos utilizadores, de armazenar estes dados e, por outro lado, uma ingerência nos direitos fundamentais do respeito pela vida privada e da proteção dos dados pessoais;

v. a circunstância de a conservação de dados de tráfego e de dados de localização para fins policiais ser suscetível de violar o direito ao respeito pelas comunicações, consagrado no art. 7.º da Carta, e de a mera conservação de tais dados pelos prestadores de serviços de comunicações eletrónicas comportar riscos de abuso e de acesso ilícito.

Considerou-se, assim, que a posição da jurisprudência da União Europeia nada alterou após o Acórdão n.º 268/2022.

Começando por analisar as normas dos arts. 4.º e 6.º da Lei n.º 32/2008, determina o Tribunal as diferenças, da seguinte forma:

A redação anterior o legislador não prescrevia a necessidade de o armazenamento de dados ocorrer no território da União Europeia, pondo em causa a efetividade dos direitos contidos nos preceitos constitucionais citados, admitindo que tais dados pudessem ser conservados em países não sujeitos à fiscalização por autoridade administrativa independente, não dando guarida à necessidade de determinação do seu armazenamento em local onde sejam efetivas as garantias constitucionais de proteção por parte de tal autoridade. Tal consideração foi suficiente para o Tribunal Constitucional concluir, sem mais, pela inconstitucionalidade de tal norma, por violação do direito à autodeterminação informativa, consagrado nos citados n.os 1 e 4 do artigo 35.º da Constituição, lidos e aplicados em conjugação com os preceitos de DUE pertinentes.

Pelo contrário, o n.º 1 do artigo 4.º do Decreto n.º 91/XV prevê que a conservação dos dados por parte dos fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações deve ser feito em Portugal ou no território de outro Estado-Membro da União Europeia. Como tal, se a conservação dos dados passa a ser feita em território em cujas jurisdições são assegurados níveis de proteção dos dados materialmente equivalentes àqueles que decorrem da Constituição, em especial do seu artigo 35.º, deixa de haver motivo para se manter o juízo de inconstitucionalidade vertido no Acórdão n.º 268/2022. Que é o mesmo que dizer: a alteração preconizada por esta norma, indo ao encontro das condições de admissibilidade elencadas pelo Tribunal Constitucional, não padece de inconstitucionalidade por violação do artigo 35.º, n.os 1 e 2, da Constituição.

As novidades mais assinaláveis do artigo 6.º, na versão ora proposta, passam, como já foi adiantado, pelo estabelecimento de regras diferenciadas em função das diferentes cate-

gorias de dados. Assim, o período de conservação para os dados de base, definidos no n.º 1 – uma vez que este se refere, na alínea a), *aos dados relativos à identificação civil dos assinantes ou utilizadores de comunicações publicamente disponíveis ou de uma rede pública de comunicações; na alínea* b), *aos demais dados de base; e, na alínea* c), *aos endereços de protocolo IP atribuídos à fonte de uma ligação –, continua a ser de um ano a contar da data da conclusão da comunicação. Acrescente-se que, mesmo em relação aos endereços de protocolo IP dinâmicos, o TJUE se pronunciou no sentido de que «as medidas nacionais que estabeleçam a sua conservação generalizada, mesmo restringindo os direitos consagrados nos artigos 7.º e 8.º da CDFUE (respeito pela vida privada e familiar; proteção de dados pessoais), deve ter-se por compatível com o direito da União Europeia, por cumprir o crivo da proporcionalidade (Acórdão* La quadrature du net, cit., *n.º 152)» (cf. Acórdão n.º 268/2022, 17.3., bem como, ainda, o Acórdão* Commissioner of An Garda Síochána, cit., *n.os 70/74). Também este Tribunal considerou, no mesmo aresto (17.4.) – como foi já visto –, que a obrigação de conservação de dados de base – incluindo de endereços de protocolo IP dinâmicos relativos à fonte de uma comunicação –, pelo período de um ano, não é em si mesma inconstitucional.*

Os dados de tráfego e de localização passam a ser conservados (apenas) pelo prazo de três meses a contar da data da conclusão da comunicação, sendo esse período prorrogado até seis meses desde que o seu titular não se tenha oposto à prorrogação da conservação (n.º 2). Em todo o caso, a prorrogação dos prazos de conservação pode ir até ao limite máximo de um ano, mediante autorização judicial, requerida pelo Procurador-Geral da República (n.º 3). Este artigo 6.º passou a ter um regime bastante mais completo e densificado, não sendo, todavia, evidente que os restantes números relevem, pelo menos autonomamente, para a questão de constitucionalidade:

– o n.º 4 determina que as prorrogações do prazo de conservação se devem limitar «ao estritamente necessário para a prossecução da finalidade prevista no n.º 1 do artigo 3.º, devendo cessar logo que se confirme a desnecessidade da sua conservação»;

– o n.º 5 dispõe que as entidades fornecedoras de serviços de comunicações eletrónicas não podem aceder aos dados conservados, salvo nos casos previstos na lei ou definidos contratualmente com o cliente;

– o n.º 6, por fim, estabelece que a autorização judicial prevista no n.º 3 compete a uma formação das secções criminais do Supremo Tribunal de Justiça, com a composição aí prevista.

Nada de essencial mudou quanto aos diversos números e alíneas do artigo 4.º (com exceção do n.º 1), pelo que a argumentação se mantém incólume. E a nova regulamentação

vertida no Decreto em apreço não obedece, de forma patente, aos condicionalismos plasmados – de forma cristalina, repetimos – neste ponto do Acórdão, que nem sequer menciona o prazo de conservação dos dados de tráfego e de localização como obstáculo à constitucionalidade das normas sindicadas.

O legislador limitou-se a restringir, para estas categorias de dados, o prazo de conservação: esse prazo era de um ano, passando agora a ser de três meses, prorrogável para seis meses e, no limite, para um ano, mediante autorização judicial. Todavia, deixou incólume o potencial âmbito subjetivo das normas, sendo precisamente aí que reside a desconformidade constitucional.

Os limites do princípio da proporcionalidade – seja o da necessidade seja o da proporcionalidade em sentido estrito – não foram superados pelo legislador; para que tal tivesse acontecido, não se revela suficiente a limitação temporal levada a cabo, impondo-se inelutavelmente que tivesse sido realizada uma limitação do âmbito subjetivo das normas. Não o tendo feito, as exigências constitucionais – paralelas às múltiplas indicações do DUE no mesmo sentido – não foram respeitadas, mantendo-se os dados da quase totalidade da população, numa base de generalidade e indiferenciação. O que vale por dizer, como possíveis suspeitos da prática de crimes (realce nosso).

No que concerne à base de dados de tráfego e localização, entendeu o Tribunal:

A conservação de tais dados, no que se refere aos dados de tráfego e de localização, cria evidentes possibilidades de extrapolação dos mesmos, com riscos claros e um enorme potencial de lesividade – designadamente de lesões aos direitos (fundamentais) à reserva da intimidade da vida privada e à autodeterminação comunicacional –, sendo por esta razão que a desproporcionalidade de tais medidas implica a sua inconstitucionalidade. Mas apresenta uma reserva:

Note-se, porém, que, atenta a vinculação do Tribunal ao pedido formulado, a apreciação da constitucionalidade levada a cabo nos presentes autos cinge-se única e exclusivamente à base de dados emergente da Lei n.º 32/2008, de 17 de julho – não se pronunciando este Tribunal quanto à viabilidade constitucional de acesso pelas autoridades de investigação criminal a dados conservados pelas operadoras em cumprimento de outras normas legais.

Parece-nos, pois, que deixa antever a conformidade constitucional quando no cumprimento de mandado de ordem judiciária.

O art. 9.º do Decreto n.º 91/XV em apreço manteve a regra segundo a qual a transmissão dos dados só pode ser autorizada por despacho fundamentado do juiz de instrução (n.º 1), em cumprimento dos demais requisitos previstos neste

número. Todavia, e por forma a ultrapassar o juízo de inconstitucionalidade, os *titulares dos dados passam a ser notificados de que os seus dados foram acedidos pelos órgãos competentes em matéria de investigação criminal*, estando agora em condições de exercer um controlo efetivo sobre o acesso a tais dados, em particular com a possibilidade de, sendo esse o caso, efetivar um controlo jurisdicional sobre a licitude e a regularidade do acesso. Assim, as exigências presentes na fundamentação do aresto deste Tribunal – bem como as do TJUE, tal como assinaladas em tal Acórdão – parecem ter sido cumpridas pelo legislador parlamentar, no Decreto submetido à apreciação do Tribunal Constitucional.

Ora, com as novas regras, passa a garantir-se que o despacho do juiz de instrução que autoriza a transmissão das diferentes categorias de dados é notificado ao titular dos dados, em princípio no prazo de 10 dias a contar da sua prolação (n.º 7 do artigo 9.º). E ainda que o n.º 8 permita ao Ministério Público – por entender que tal notificação pode pôr em risco a investigação, dificultar a descoberta da verdade ou criar perigo para a vida, para a integridade física ou psíquica ou para a liberdade dos participantes processuais, das vítimas do crime ou de outras pessoas – solicitar ao juiz de instrução o protelamento da notificação, a norma assegura que ela será feita no prazo máximo de 10 dias a contar da data em que for proferido o despacho de encerramento desta fase processual.

No entanto, segundo o Tribunal Constitucional, não se afigura que tal restrição, filtrada pelos requisitos decorrentes do princípio da proporcionalidade, consagrados no n.º 2 do art. 18.º da Constituição, ultrapasse tais requisitos: *ponderando, nomeadamente, os motivos que o Ministério Público terá de invocar para requerer o protelamento, o nosso entendimento é de que a restrição não se revela excessiva. Olhando para as várias dimensões do princípio da proporcionalidade, o protelamento afigura-se ser uma medida apta aos fins que pretende atingir, não sendo tão-pouco violadora da dimensão da necessidade ou exigibilidade nem da proporcionalidade em sentido estrito, uma vez que, em face dos benefícios esperados com tal medida, num juízo de ponderação, parece justificar-se a compressão aos direitos fundamentais em causa que, em todo o caso, não deixa de acarretar – não se vislumbrando opção menos restritiva para aquele direito fundamental sem que venha acompanhada de uma substancial redução de eficácia quanto ao objetivo visado. Como, aliás, foi dito no Acórdão n.º 268/2022: «(…) a notificação ao visado de que tal transmissão ocorreu – a partir do momento em que tal comunicação não seja já suscetível de comprometer as investigações ou de constituir risco para a integridade física ou vida de terceiros – constituiria opção menos restritiva, sem que se vislumbre qualquer redução de eficácia face aos expedientes vigentes*».

Assim, a nova redação do artigo 9.º acolhe uma solução equilibrada no que respeita à ponderação entre os interesses que justificam o acesso aos dados pelas autoridades competentes em matéria de investigação criminal e as exigências decorrentes do direito à autodeterminação informativa, previsto no artigo 35.º da Constituição e, ainda, do princípio da proibição do excesso, tal como plasmadas no artigo 18.º, n.º 2; quer, ainda, do direito a uma tutela jurisdicional efetiva, previsto no artigo 20.º, n.º 1, da Lei Fundamental.

E desta forma foi este o dispositivo:

(a) *Pronunciar-se pela inconstitucionalidade da norma constante do artigo 2.º do Decreto n.º 91/XV, da Assembleia da República, publicado no* Diário da Assembleia da República*, n.º 26, II Série A, de 26 de outubro de 2023, e enviado ao Presidente da República para promulgação como lei, na parte em que altera o artigo 4.º da Lei n.º 32/2008, de 17 de julho, conjugado com o artigo 6.º da mesma Lei, quanto aos dados previstos no n.º 2 do mencionado artigo 6.º, por violação do disposto nos números 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, todos da Constituição;*

(b) *Não se pronunciar pela inconstitucionalidade das demais normas cuja apreciação foi requerida.*

Também nesta decisão foram proferidos vários votos de vencido que, de uma forma resumida e sintética, determinam não se verificar qualquer inconstitucionalidade na amplitude subjetiva dos dados conservados, bem como a criação de base de dados, na medida em que já existem no nosso ordenamento jurídico meios de obtenção da prova onde tal "invasão" se verifica e não existe declaração de inconstitucionalidade, face à ponderação do interesse investigatório na criminalidade grave; exemplo paradigmático são as escutas telefónicas[17].

Conclusões

No direito penal constata-se a necessidade, permanente, em equilibrar a restrição e a defesa dos direitos fundamentais. Devemos analisar, com muito cuidado, se a necessidade da restrição satisfaz aquilo que, com a mesma, se pretende

[17] Não se pode descurar o carácter dissimulado das escutas telefónicas que lhe garante uma, quase, automática eficácia; todavia, ponderadas a proporcionalidade, a necessidade e a adequação, são consideradas um meio legítimo de obtenção da prova.

Sobre a temática das escutas telefónicas, ver o nosso anterior trabalho *Escutas Telefónicas. Regime Processual Penal,* Quid Iuris, 2009.

proteger ou prevenir. Esta tarefa, tão importante, deve ser feita por todos, mas especialmente pelo legislador e aplicador da lei. Nunca podemos deixar de estar atentos, quer por via académica, institucional ou mesmo social. A nossa atenção é um instrumento de controlo das referidas atividades que também são o garante do Estado de Direito democrático.

Seguindo as palavras de HUGO LUZ SANTOS: *O princípio da legalidade digital, bem como o princípio da ética digital, assimilam-se, neste ponto, ao princípio da vinculação do fim (Zweckbindung), que se arvora em limite intransponível no processo penal. Mesmo no processo penal do Great Reset [novo mundo]*[18].

[18] HUGO LUZ SANTOS, "Processo Penal e Inteligência Artificial: Rumo a um Direito (Processual) Penal da Segurança Máxima?", in *Revista Brasileira de Direito Processual Penal*, vol. 8, n.º 2, mai./ago. 2022, pp. 767-821, *https://doi.org/10.22197/rbdpp.v8i2.709*.