5

IMPEDIRÁ O ACÓRDÃO DO TRIBUNAL CONSTITUCIONAL N.º 268/2022 A OBTENÇÃO E A VALORAÇÃO, PARA FINS DE INVESTIGAÇÃO CRIMINAL, DE METADADOS CONSERVADOS PELOS FORNECEDORES DE SERVIÇOS DE COMUNICAÇÕES ELETRÓNICAS AO ABRIGO DA LEI ATUALMENTE EM VIGOR?[1]

Duarte Rodrigues Nunes[2]

[1] **Como citar este artigo científico**. NUNES, Duarte Rodrigues. Impedirá o Acórdão do Tribunal Constitucional n.º 268/2022 a obtenção e a valoração, para fins de investigação criminal, de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas ao abrigo da lei atualmente em vigor? In: **Revista Amagis Jurídica**, Belo Horizonte, Ed. Associação dos Magistrados Mineiros, v. 15, n. 2, p. 127-184, maio-ago. 2023.

[2] Professor associado convidado da Universidade Europeia. Professor convidado da Universidade Lusíada de Angola. Doutor em Direito pela Faculdade de Direito da Universidade de Lisboa. Jurisconsulto. Investigador integrado do Centro de Investigação de Direito Penal e Ciências Criminais e não integrado do Centro de Investigação Jurídica do Ciberespaço, ambos da Faculdade de Direito da Universidade de Lisboa. Conferencista. Autor de seis monografias jurídicas: Os meios de obtenção de prova da Lei do Cibercrime (Coimbra: Gestlegal, 2018; reimpressão, 2020; 2.ª edição, 2021), Revistas e Buscas no Código de Processo Penal (Coimbra: Gestlegal, 2019), O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada (Dissertação de Doutoramento, Coimbra, Ed. Gestlegal, 2019), Os crimes previstos na Lei do Cibercrime (Coimbra: Gestlegal, 2020; reimpressão, 2021), Curso de Direito Penal, Parte Geral, Tomo I (Coimbra: Gestlegal, 2021; 2.ª edição, 2022) e Curso de Direito Processual Penal, Tomo I (em publicação). O autor exerceu, entre 2005 e 2022 as funções de Juiz de Direito, estando atualmente em situação de licença sem vencimento. *e-mail*: duarterodriguesnunes@gmail.com

RESUMO

O Tribunal Constitucional, através do seu Acórdão n.º 268/2022, declarou a inconstitucionalidade, com força obrigatória geral, das normas do artigo 4.º, conjugado com o artigo 6.º, e do artigo 9.º, todos da Lei n.º 32/2008, de 27 de julho. No presente artigo, analisam-se, de forma crítica, a decisão e os respetivos fundamentos, bem como é proposto um fundamento jurídico alternativo à luz da lei vigente (que não tenha sido abrangida pelo aresto do Tribunal Constitucional) para a conservação de metadados e para a sua utilização em processos penais, dado que se trata de um meio de obtenção de prova cada vez mais essencial para o apuramento da verdade material, inclusivamente relativamente a crimes particularmente graves e a formas de criminalidade extremamente danosas para os direitos fundamentais dos cidadãos e de investigação muito difícil. Visa-se, deste modo, permitir a utilização deste relevantíssimo meio de obtenção de prova em processos em curso e, acima de tudo, obstar à eventual reversão de condenações transitadas em julgado e as consequentes absolvições materialmente injustas e insuficiente proteção dos direitos fundamentais a que se reconduzem os bens jurídico-penais tutelados pelas incriminações concretamente em causa.

ABSTRACT

The Constitutional Court, through its judgment no. 268/2022, declared article 4, in conjunction with article 6, and article 9, all of Law no. 32/2008, of 27th July, unconstitutional. In this article, the decision and its grounds are critically analysed. An alternative legal basis (in the light of the law still in force) for metadata retention and for its use in criminal proceedings is also proposed, given that it is a means of obtaining evidence that is increasingly essential for the establishment of material truth, including in relation to particularly serious crimes and forms of crime that are extremely harmful to the fundamental rights of citizens and whose investigation is very difficult. The purpose of this article is, therefore, to allow the use of this very relevant means of obtaining evidence in ongoing proceedings and, above all, to prevent eventual reversals of final and unappealable convictions and the consequent unfair acquittals and insufficient protection of the fundamental rights violated through the commission of the criminal offenses specifically under consideration.

de 15 de março, através da Lei N.º 32/2008, de 17 de junho. III A declaração de invalidade da Diretiva 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de março pelo Tribunal de Justiça da União Europeia. IV A declaração de inconstitucionalidade com força obrigatória geral dos artigos 4.º, 6.º e 9.º (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) da Lei N.º 32/2008, de 17 De Julho. V A admissibilidade da utilização de metadados na investigação criminal apesar da declaração de inconstitucionalidade por via do Acórdão do Tribunal Constitucional N.º 268/2022. VI Conclusões. Referências.

I COLOCAÇÃO DO PROBLEMA[3]

O Tribunal Constitucional (TC)[4] declarou inconstitucionais, com força obrigatória geral:

a) a norma constante do artigo 4.º da Lei n.º 32/2008[5], conjugada com o artigo 6.º da mesma lei, por violação do disposto nos artigos 35.º, n.ºs 1 e 4, e 26.º, n.º 1, em conjugação com o artigo 18.º, n.º 2, todos da Constituição da República Portuguesa (CRP)[6]; e

[3] O presente artigo, corresponde, no essencial, ao artigo que publicámos com o mesmo título na Revista do Ministério Público, n.º 170, Sindicato dos Magistrados do Ministério Público, Lisboa, 2022. Procedemos a algumas alterações no texto (que não alteram o sentido das opiniões que então defendemos e continuamos a defender), aditámos no final as referências bibliográficas e jurisprudenciais e, ao longo do texto, referências legislativas (e respetivo endereço eletrónico onde podem ser consultadas) e relativas à designação dos tribunais portugueses (que, no texto original, surgem identificados apenas com as suas siglas).

[4] Acórdão n.º 268/2022 (com um voto de vencido).

[5] Lei n.º 32/2008, de 17 de julho, texto integral está disponível no endereço <*https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?artigo_id=1264A0001&nid=1264&tabela=leis&pagina=1&ficha=1&so_miolo=&nversao=#artigo*|>.

[6] O texto integral da Constituição da República Portuguesa está disponível no endereço <*https://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx*>.

b) a norma constante do artigo 9.º da Lei n.º 32/2008 (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 nos artigos 35.º, n.º 1, e 20.º, n.º 1, em conjugação com o artigo 18.º, n.º 2, todos da CRP.

O Acórdão n.º 268/2022 foi prolatado no âmbito de um pedido de declaração de inconstitucionalidade dos artigos 4.º, 6.º e 9.º da Lei n.º 32/2008, em sede de fiscalização abstrata sucessiva à luz do artigo 281.º da CRP, formulado pela Provedora da Justiça.

A requerente invocava a violação do Direito da União Europeia (artigos 7.º, 8.º e 52.º, n.º 1, da CDFUE[7]), do direito à reserva da intimidade da vida privada e familiar (artigo 26.º, n.º 1, da CRP), do princípio da proporcionalidade (artigo 18.º, n.º 2, da CRP), do sigilo das comunicações (artigo 34.º da CRP) e do direito a uma tutela jurisdicional efetiva (artigo 20.º, n.º 1, da CRP).

O TC apreciou a constitucionalidade das normas referidas supra em a) e b) também à luz do direito à autodeterminação informacional, tutelado pelo artigo 35.º da CRP, e do direito ao livre desenvolvimento da personalidade, tutelado pelo artigo 26.º, n.º 1, da CRP, pois considerou que o princípio do pedido não obsta a que o TC possa declarar a inconstitucionalidade das normas cuja apreciação foi requerida com fundamento diverso daqueles cuja violação foi alegada, invocando, para tal, o disposto no artigo 51.º, n.º 5, da Lei Orgânica do Tribunal Constitucional[8] (LTC).

[7] Tendo em conta a declaração de invalidade da Diretiva 2006/24/CE pelo Tribunal de Justiça da União Europeia (TJUE) através do seu Acórdão 8 de abril de 2014, *Digital Rights Ireland Ltd e Kärntner Landesregierung*.

[8] Lei n.º 28/82, de 15 de novembro, cujo texto integral está disponível no endereço *<https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=423&tabela=leis>*.

A declaração da inconstitucionalidade dos artigos 4.º (conjugada com o artigo 6.º) e 9.º da Lei n.º 32/2008 veio suscitar a questão da admissibilidade, ou não, da obtenção e valoração, nos processos em curso, de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações (metadados) e que tenham sido conservados pelos respetivos operadores e das provas obtidas através desses metadados. E, ainda mais grave, veio abrir a possibilidade[9] de, sendo intentados recursos de revisão ao abrigo do artigo 449.º, n.º 1, alíneas e) e f), do Código de Processo Penal (CPP)[10], caso eles sejam julgados procedentes, serem revertidas condenações transitadas em julgado em processos nos quais, em observância de todas as garantias e esgotados todos os mecanismos de recurso de que os arguidos tenham decidido lançar mão, se provou, para além da dúvida razoável, o cometimento do crime ou dos crimes pelos quais foram condenados. Com todas as consequências que daí possam advir (e que são tão mais gravosas nos casos de condenações por crimes graves) e que recensearemos infra.

A finalidade do presente estudo não é apontar propostas relativamente aos termos da nova legislação que não poderá deixar de ser aprovada, atenta a essencialidade da obtenção de metadados conservados pelos fornecedores de serviços de comunicações eletrónicas para a investigação criminal de não poucos crimes (e muitos deles extremamente graves e de dificílima investigação), mas sim formular propostas ao nível da obtenção e valoração dos metadados ao abrigo da legislação em vigor que não tenha sido declarada inconstitucional pelo TC (caso tal se mostre possível), a fim de permitir a sua obtenção e valoração nos processos em curso e obstar à reversão de condenações transitadas em julgado. Todavia, uma tal solução, a revelar-se possível, será sempre uma solução

[9] Pelo menos em abstrato, pois, tendo em conta o que referiremos infra, consideramos que os recursos de revisão que venham a ser intentados com base no Acórdão n.º 268/2022 do TC não poderão deixar de improceder.

[10] O texto integral do Código de Processo Penal está disponível no endereço *<https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=199&tabela=leis>*.

provisória e exigirá uma intervenção legislativa tão rápida quanto possível.

II A TRANSPOSIÇÃO DA DIRETIVA 2006/24/CE, DO PARLAMENTO EUROPEU E DO CONSELHO, DE 15 DE MARÇO, ATRAVÉS DA LEI N.º 32/2008, DE 17 DE JUNHO

No dia 4 de agosto de 2009, entrou em vigor a Lei n.º 32/2008[11], que transpôs para a nossa ordem jurídica a Diretiva 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de março[12], 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 (metadados).

A Diretiva 2006/24/CE visou harmonizar as disposições dos Estados-Membros relativas às obrigações dos fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações em matéria de conservação de dados de tráfego, dos dados de localização relativos pessoas singulares e/ou a pessoas coletivas e dos dados conexos necessários para identificar o assinante ou o utilizador registado por eles gerados ou tratados, tendo em vista garantir a disponibilidade desses dados para efeitos de investigação, de deteção e de repressão de crimes graves, tal como definidos no Direito nacional de cada Estado-Membro.

Esta Diretiva veio prever a obrigação de os Estados-Membros tomarem medidas para garantir a conservação dos dados necessários para (1) encontrar e identificar a fonte e/ou o destino de uma comunicação, (2) identificar a data, a hora e a duração de uma

[11] De acordo com o artigo 18.º desta Lei, a mesma entraria em vigor 90 dias após a publicação da portaria a que se refere o n.º 3 do artigo 7.º, sendo que a portaria em causa é a Portaria n.º 469/2009, de 6 de maio, que, nos termos do seu artigo 7.º, entrou em vigor no dia seguinte ao da sua publicação. O texto integral da Portaria n.º 469/2009 está disponível no endereço <*https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1265&tabela=leis&so_miolo=*>.

[12] Disponível em: <*https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32006L0024*>.

comunicação, (3) identificar o tipo de comunicação, (4) identificar o equipamento de telecomunicações dos utilizadores ou o que se considera ser o seu equipamento e (5) identificar a localização do equipamento de comunicação móvel (incluindo no caso de chamadas telefónicas falhadas), quando gerados ou tratados e armazenados (no caso de dados telefónicos) ou registados (no caso de dados da Internet) por fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações que estejam sob a jurisdição do Estado-Membro em questão, no contexto da oferta de serviços de comunicação, mas exclui expressamente do seu âmbito de aplicação os dados de conteúdo de comunicações (artigos 1.º, n.º 2, e 5.º, n.º 2).

De acordo com o seu artigo 1.º, a Lei n.º 32/2008 regula a conservação e a transmissão dos dados de tráfego e de localização relativos a pessoas singulares e a pessoas coletivas, bem como dos dados conexos necessários para identificar o assinante ou o utilizador registado, para fins de investigação, deteção e repressão de crimes graves por parte das autoridades competentes, não contemplando, contudo, a conservação de dados que revelem o conteúdo das comunicações, que é proibida, sem prejuízo do disposto na Lei n.º 41/2004, de 18 de agosto[13], e na legislação processual penal relativamente à interceção e gravação de comunicações.

Como resulta do artigo 3.º, a conservação e a transmissão dos dados têm por finalidade exclusiva a investigação, deteção e repressão de crimes graves por parte das autoridades competentes, sendo obrigatória a separação dos ficheiros destinados à conservação de dados de quaisquer outros ficheiros para outros fins e não podendo o titular dos dados opor-se à respetiva conservação e transmissão.

Nos termos dos artigos 4.º e 5.º, os fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações estavam obrigados a conservar (1) os dados necessários para encontrar e identificar a fonte de uma

[13] O texto integral da Lei n.º 41/2004 está disponível no endereço <*https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=707&tabela=leis&so_miolo=*>.

comunicação, (2) os dados necessários para encontrar e identificar o destino de uma comunicação, (3) os dados necessários para identificar a data, a hora e a duração de uma comunicação, (4) os dados necessários para identificar o tipo de comunicação, (5) os dados necessários para identificar o equipamento de telecomunicações dos utilizadores, ou o que se considera ser o seu equipamento e (6) os dados necessários para identificar a localização do equipamento de comunicação móvel, incluindo os dados telefónicos e da Internet relativos a chamadas telefónicas falhadas quando gerados, tratados e/ou armazenados por esses mesmos fornecedores de serviços de comunicações eletrónicas, mas não os dados relativos a chamadas não estabelecidas.

O prazo de conservação era de um ano (cfr. artigo 6.º)[14] e, no que tange à proteção e à segurança dos dados conservados, de acordo com o artigo 7.º, n.ºs 1 e 2, os fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações estão obrigados a:

a) conservar os dados referentes às categorias previstas no artigo 4.º por forma a que possam ser transmitidos imediatamente, mediante despacho fundamentado do Juiz, às autoridades competentes;

b) garantir que os dados conservados sejam da mesma qualidade e estejam sujeitos à mesma proteção e segurança que os dados na rede;

c) tomar as medidas técnicas e organizativas adequadas à proteção dos dados previstos no artigo 4.º contra a destruição acidental ou ilícita, a perda ou a alteração acidental e o armazenamento, tratamento, acesso ou divulgação não autorizados ou ilícitos;

[14] Nos termos do artigo 12.º, n.ºs 1, alínea b), 2 e 3, sem prejuízo da responsabilidade criminal a que haja lugar nos termos da lei, o incumprimento do prazo de conservação previsto no artigo 6.º constitui uma contraordenação punível com uma coima entre 1500,00 € e 50 000,00 €, quando o agente seja uma pessoa singular, ou entre 5000,00 € e 10 000 000,00 €, quando o agente seja uma pessoa coletiva, sendo a tentativa e a negligência puníveis.

d) tomar as medidas técnicas e organizativas adequadas para garantir que apenas pessoas especialmente autorizadas tenham acesso aos dados referentes às categorias previstas no artigo 4.º;

e) destruir os dados no final do período de conservação, exceto os dados que tenham sido preservados por ordem do Juiz; e

f) destruir os dados que tenham sido preservados, quando tal lhe seja determinado por ordem do Juiz.

Isto, devendo os dados referentes às categorias previstas no artigo 4.º, à exceção dos dados relativos ao nome e endereço dos assinantes, permanecer bloqueados (*i. e.*, encriptados) desde o início da sua conservação e só podendo ser desbloqueados (*i. e.*, desencriptados) para efeitos de transmissão, nos termos da Lei n.º 32/2008, às autoridades competentes, que, nos termos do artigo 2.º, n.º 1, alínea f), são as autoridades judiciárias [na aceção do artigo 1.º, alínea b)], do CPP: Juiz, Juiz de Instrução Criminal (JIC) e Ministério Público (MP) e as autoridades de polícia criminal (APC) da Polícia Judiciária (PJ), Guarda Nacional Republicana (GNR), Polícia de Segurança Pública (PSP), Polícia Judiciária Militar (PJM), Serviço de Estrangeiros e Fronteiras (SEF) e Polícia Marítima.

Para garantir a efetividade do cumprimento das obrigações relativas à conservação e à transmissão dos dados às autoridades competentes, nos termos do artigo 12.º, n.ºs 1, alíneas a) a c), 2 e 3, sem prejuízo da responsabilidade criminal a que haja lugar nos termos da lei, a não conservação das categorias dos dados previstas no artigo 4.º, o incumprimento do prazo de conservação previsto no artigo 6.º e a não transmissão dos dados às autoridades competentes, quando autorizada nos termos do disposto no artigo 9.º constituem contraordenação punível com uma coima entre 1500,00 € e 50 000,00 €, quando o agente seja uma pessoa singular, ou entre 5000,00 € e 10 000 000,00 €, quando o agente seja uma pessoa coletiva, sendo a tentativa e a negligência puníveis.

A transmissão dos dados processa-se mediante comunicação eletrónica, nos termos das condições técnicas e de segurança fixadas na Portaria n.º 469/2009, que devem observar um grau de codificação e proteção o mais elevado possível, de acordo com o estado da técnica ao momento da transmissão, incluindo métodos de codificação, encriptação ou outros adequados (cfr. artigos 7.º, n.º 3, e 10.º).

Ainda no que concerne à proteção e à segurança dos dados, de acordo com os artigos 8.º e 9.º, n.º 6, a Comissão Nacional de Proteção de Dados (CNPD) (que, nos termos do artigo 7.º, n.º 5, é a autoridade pública competente para o controlo do cumprimento das regras relativas à proteção e à segurança dos dados[15]) deve manter um registo eletrónico permanentemente atualizado das pessoas especialmente autorizadas a aceder aos dados, estando os fornecedores de serviços de comunicações eletrónicas ou de uma rede pública de comunicações, por seu turno, obrigados a remeter à CNPD, por via exclusivamente eletrónica, os dados necessários à identificação das pessoas especialmente autorizadas a aceder aos dados.

Para reforçar a proteção e a segurança dos dados, o legislador criminalizou diversas condutas, sendo que, nos termos do artigo 13.º, o incumprimento de qualquer das regras relativas à proteção e à segurança dos dados previstas no artigo 7.º, o não bloqueio dos dados, nos termos previstos no n.º 2 do artigo 7.º, e o acesso aos dados por pessoa não especialmente autorizada nos termos do n.º 1 do artigo 8.º constituem crime punível com pena de prisão entre um mês e dois anos ou com pena de multa entre dez e 240 dias, sendo a penalidade agravada para o dobro dos seus limites mínimo e

[15] No entanto, na sua Deliberação n.º 1008/2017, na sequência da anulação da Diretiva 2006/24/CE pelo TJUE, a CNPD decidiu desaplicar a Lei n.º 32/2008 por violar a Carta dos Direitos Fundamentais da União Europeia (CDFUE) e o artigo 18.º, n.º 2, da CRP, como se de um Tribunal se tratasse, procedimento cuja legitimidade se nos afigura muitíssimo duvidosa. Ademais, segundo notícia publicada pelo Diário de Notícias em 15/05/2022, as bases de metadados das operadoras não são fiscalizadas pela CNPD desde a referida deliberação (*i. e.*, há cerca de cinco anos).

máximo quando o crime for cometido através de violação de regras técnicas de segurança, tiver possibilitado ao agente ou a terceiros o conhecimento de dados pessoais e/ou tiver proporcionado ao agente ou a terceiros benefício ou vantagem patrimonial. A tentativa e a negligência são puníveis.

Do mesmo modo, nos termos do artigo 12.º, n.ºs 1, alínea d), 2 e 3, sem prejuízo da responsabilidade criminal a que haja lugar nos termos da lei, o não envio dos dados necessários à identificação das pessoas especialmente autorizadas, nos termos do n.º 2 do artigo 8.º constitui uma contraordenação punível com uma coima entre 1500,00 € e 50 000,00 €, quando o agente seja uma pessoa singular, ou entre 5000,00 € e 10 000 000,00 €, quando o agente seja uma pessoa coletiva, sendo a tentativa e a negligência puníveis.

De acordo com os artigos 2.º, n.º 3, e 9.º, n.ºs 1, 2 e 4[16], a transmissão dos dados às autoridades competentes só pode ser ordenada ou autorizada por despacho fundamentado do Juiz (ou JIC), mediante requerimento do MP ou da APC competente, se houver razões para crer que a diligência é indispensável para a descoberta

[16] Como sempre defendemos, consideramos que o artigo 9.º da Lei n.º 32/2008 foi tacitamente revogado pelos artigos 12.º e ss. da Lei n.º 109/2009, de 15 de setembro (cfr. NUNES, 2019a, p. 563-564; e também em NUNES, 2021b, p. 65 e ss.), entendimento também perfilhado por Mesquita (2010, p. 110, 111 [nota 60], 113-114 e 123), e pelos Acórdãos do Tribunal da Relação de Lisboa (TRL) de 22/01/2013, do Tribunal da Relação de Coimbra (TRC) de 26/02/2014 e do Tribunal da Relação de Évora (TRE) de 06/01/2015, sendo que, no Acórdão do TRL de 21/11/2018, embora começando por se afirmar a adesão à tese maioritária, considerou-se que o artigo 14.º da Lei n.º 109/2009 permite a obtenção de dados conservados à luz da Lei n.º 32/2008 fora dos casos em que esteja em causa a investigação de um crime subsumível ao conceito de "crime grave" do artigo 2.º, n.º 1, alínea g), desta última lei. Contudo, o entendimento maioritário era no sentido de que o artigo 9.º da Lei n.º 32/2008 prevalecia sobre o regime dos artigos 12.º e ss. da Lei n.º 109/2009, embora, com a declaração de inconstitucionalidade com força obrigatória geral do artigo 9.º da Lei n.º 32/2008 (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 via do Acórdão do TC n.º 268/2022, tal entendimento deixou de ter qualquer apoio na lei vigente.

da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter no âmbito da investigação, deteção e repressão de crimes graves, que, nos termos do artigo 2.º, n.º 1, alínea g), são os crimes de terrorismo[17], criminalidade violenta[18], criminalidade altamente organizada[19], sequestro, rapto e tomada de reféns, crimes contra a identidade cultural e integridade pessoal, contra a segurança do Estado, falsificação de moeda ou de títulos equiparados a moeda, contrafação de cartões ou outros dispositivos de pagamento, uso de cartões ou outros dispositivos de pagamento contrafeitos, aquisição de cartões ou outros dispositivos de pagamento contrafeitos, atos preparatórios da contrafação e crimes abrangidos por convenção sobre segurança da navegação aérea ou marítima, devendo a decisão judicial de transmitir os dados 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 proteção do segredo profissional.

Nos termos do artigo 9.º, n.º 3, só pode ser autorizada a transmissão de dados relativos ao suspeito ou ao arguido, 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 de arguido, ou a vítima de crime, mediante o respetivo consentimento (efetivo ou presumido).

A Lei exige, igualmente, que os fornecedores de serviços de comunicações eletrónicas ou de uma rede pública de comunicações

[17] Na aceção do artigo 1.º, alínea i), do CPP: as condutas que integram os crimes de organizações terroristas, terrorismo, terrorismo internacional e financiamento do terrorismo.

[18] Na aceção do artigo 1.º, alínea j), do CPP (que inclui a criminalidade especialmente violenta, a que se refere a alínea l) do mesmo normativo): as condutas que dolosamente se dirigirem contra a vida, a integridade física, a liberdade pessoal, a liberdade e autodeterminação sexual ou a autoridade pública e forem puníveis com pena de prisão de máximo igual ou superior a 5 anos.

[19] Na aceção do artigo 1.º, alínea m), do CPP: as condutas que integrarem crimes de associação criminosa, tráfico de órgãos humanos, tráfico de pessoas, tráfico de armas, tráfico de estupefacientes ou de substâncias psicotrópicas, corrupção, tráfico de influência, participação económica em negócio ou branqueamento.

elaborem registos da extração dos dados transmitidos às autoridades competentes e, trimestralmente, enviem esses registos à CNPD (cfr. artigo 9.º, n.º 6).

Por fim, de acordo com o artigo 11.º, o Juiz determina, oficiosamente ou a requerimento de qualquer interessado, a destruição dos dados na posse das autoridades competentes, bem como dos dados preservados pelos fornecedores de serviços de comunicações eletrónicas ou de uma rede pública de comunicações logo que eles deixem de ser estritamente necessários para os fins a que se destinam, considerando-se que deixam de o ser quando (1) o processo penal seja arquivado nos termos do artigo 277.º, n.º 1, do CPP, (2) o arguido seja não pronunciado ou absolvido por decisão transitada em julgado, (3) o arguido seja condenado por decisão transitada em julgado, (4) ocorra a prescrição do procedimento penal ou (5) tenha lugar uma amnistia.

III A DECLARAÇÃO DE INVALIDADE DA DIRETIVA 2006/24/CE, DO PARLAMENTO EUROPEU E DO CONSELHO, DE 15 DE MARÇO PELO TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA

A Diretiva 2006/24/CE foi declarada inválida pelo TJUE, no âmbito de um reenvio prejudicial ao abrigo do artigo 267.º do TFUE através do seu Acórdão de 8 de abril de 2014, *Digital Rights Ireland Ltd e Kärntner Landesregierung*. Nesse aresto, o TJUE entendeu que a conservação dos dados referidos na Diretiva e o acesso das autoridades a esses dados restringem, de forma intensa (embora sem afetar o seu conteúdo essencial), os direitos tutelados pelos artigos 7.º e 8.º da CDFUE, sendo que, nos termos do artigo 52.º, n.º 1, da Carta, qualquer restrição ao exercício dos direitos e liberdades reconhecidos por esta deve ser prevista por lei, respeitar o conteúdo essencial desses direitos e liberdades e, por força dos ditames do princípio da proporcionalidade, só podem ser introduzidas restrições a esses direitos e liberdades se forem necessárias e corresponderem

efetivamente a objetivos de interesse geral reconhecidos pela União ou à necessidade de proteção dos direitos e liberdades de terceiros. E, nessa conformidade, o TJUE considerou que, apesar de não ocorrer qualquer restrição do conteúdo essencial dos referidos direitos fundamentais e de estar em causa a prossecução de fins legítimos (a resposta à criminalidade grave e, em última análise, a salvaguarda da segurança pública), a Diretiva restringe, de forma desproporcionada, os mencionados direitos fundamentais, uma vez que:

a) abrange, de uma forma indiscriminada, todas as pessoas que utilizam serviços de comunicações eletrónicas, incluindo, por isso, pessoas em relação às quais não existem indícios de que o seu comportamento possa ter um nexo, ainda que indireto ou longínquo, com infrações graves e não prevendo qualquer exceção quanto a pessoas cujas comunicações estejam abrangidas pela proteção do segredo profissional;

b) não exige nenhuma relação entre os dados cuja conservação está prevista e uma ameaça para a segurança pública nem limita a conservação a dados relativos a um período de tempo e/ou a uma zona geográfica determinada e/ou a um círculo de pessoas determinadas que possam estar implicadas, de uma maneira ou de outra, numa infração grave, nem de dados relativos a pessoas, cuja conservação, por outros motivos, pudesse contribuir para a prevenção, a deteção ou a repressão de infrações graves;

c) não estabelece critérios objetivos que permitam delimitar o acesso das autoridades nacionais competentes aos dados e a sua utilização posterior para prevenir, detetar ou agir penalmente contra infrações suscetíveis de ser consideradas suficientemente graves à luz da amplitude e da gravidade da ingerência nos direitos fundamentais consagrados nos artigos 7.º e 8.º da CDFUE para justificar uma tal ingerência;

d) no que tange ao acesso das autoridades nacionais competentes aos dados e à sua utilização posterior, não limita o acesso e a utilização posterior dos dados em causa a fins de prevenção e de deteção de infrações graves delimitadas com precisão ou de ações penais contra as mesmas nem estabelece critérios objetivos que permitam limitar o número de pessoas com autorização de acesso e de utilização posterior dos dados conservados ao estritamente necessário à luz do objetivo prosseguido;

e) não submete o acesso aos dados conservados pelas autoridades nacionais competentes a um controlo prévio efetuado por um órgão jurisdicional ou por uma entidade administrativa independente cuja decisão vise limitar o acesso aos dados e a sua utilização ao estritamente necessário para se alcançar o objetivo prosseguido e ocorra na sequência de um pedido fundamentado destas autoridades, apresentado no âmbito de procedimentos de prevenção, de deteção ou de uma ação penal, sendo que também não foi prevista uma obrigação precisa de os Estados-Membros estabelecerem tais limitações;

f) no que respeita à duração da conservação dos dados, não procede a qualquer distinção entre as categorias de dados em função da sua eventual utilidade relativamente ao objetivo prosseguido ou em função das pessoas em causa e situa essa duração entre um mínimo de seis meses e um máximo de vinte e quatro meses, sem que se especifique que a determinação do período de conservação se deve basear em critérios objetivos, a fim de garantir que se limita ao estritamente necessário; e

g) quanto à segurança e à proteção dos dados conservados pelos fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, não se estabelece nem se

> prevê uma obrigação precisa de os Estados-Membros estabelecerem regras específicas e adaptadas à grande quantidade de dados cuja conservação é imposta, ao caráter sensível desses dados e ao risco de acesso ilícito aos mesmos, não garante a aplicação pelos referidos fornecedores de um nível particularmente elevado de proteção, não garante a destruição definitiva dos dados no termo do período de conservação dos mesmos e também não impõe que os dados em causa sejam conservados no território da União Europeia (pelo que não se pode considerar que esteja plenamente garantida a fiscalização, por uma entidade independente, expressamente exigida pelo artigo 8.º, n.º 3, da CDFUE, do respeito das exigências de proteção e de segurança).

Na sequência deste Acórdão do TJUE, passou a discutir-se, entre nós, se a Lei n.º 32/2008 era, ou não, incompatível com o Direito da União Europeia e se, consequentemente, a conservação de dados à luz dessa Lei é, ou não, admissível à luz, quer da CRP quer da CDFUE.

Assim, uma parte da doutrina e da jurisprudência consideravam que o Acórdão do TJUE não impede a conservação de dados nem o acesso a esses dados, à luz da Lei n.º 32/2008, pois tratou-se de um Acórdão proferido em sede de reenvio prejudicial e, como tal, sem força obrigatória geral e apenas vinculativo para os Estados em causa [ao contrário do que sucederia se a Diretiva tivesse sido declarada inválida no âmbito de recurso de anulação nos termos do artigo 263.º do Tratado sobre o Funcionamento da União Europeia (TFUE)] e, sobretudo, porque a Lei n.º 32/2008 cumpre todos os requisitos que o TJUE entendeu que a Diretiva 2006/24/CE não observa[20]. Igualmente se entendeu que ainda que a Lei n.º

[20] Cfr. Nunes (2019a, p. 558 e ss.), Correia (2014, p. 38), Pinho (2018, *passim*, embora entendendo que a Lei n.º 32/2008 terá de ser alvo de reformas, mas por força da entrada em vigor do RGPD), Milheiro (2019, p. 840-841); Cabreiro (2014), e Acórdãos do TC n.º 420/2017 e do TRL de 28/11/2018.

32/2008 seja o instrumento de transposição da Diretiva 2006/24/CE para a ordem jurídica portuguesa, a declaração de invalidade da Diretiva pelo TJUE não implicava *ipso facto* a invalidade da Lei n.º 32/2008 (que passou a valer como uma lei nacional autónoma), que, contudo, deveria ser alvo de alteração, a fim de a conformar ao disposto na CDFUE e à jurisprudência do TJUE[21].

Mas também não faltou quem, por força da jurisprudência do TJUE, considerasse que a Lei n.º 32/2008 era inconstitucional por violar a CDFUE e, por isso, os Tribunais portugueses estavam impedidos de a aplicar[22] e quem não descartasse a possibilidade de a Lei n.º 32/2008 vir a ser considerada inconstitucional em sede de fiscalização da constitucionalidade (como veio, efetivamente, a suceder), por violação do princípio da proporcionalidade (cfr. MARTINS, 2017, p. 512).

Trata-se, todavia, de uma questão ultrapassada, por força da declaração de inconstitucionalidade, com força obrigatória geral, dos artigos. 4.º, 6.º e 9.º (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) da Lei n.º 32/2008 por meio do Acórdão do TC n.º 268/2022, apenas valendo os argumentos então esgrimidos para apreciar criticamente o decidido neste aresto e os respetivos fundamentos.

[21] Cfr. Acórdão do TRE de 22/02/2022.

[22] Cfr. Ramalho; Coimbra (2015, p. 1.039 e ss.), Ramos (2022, p. 261 e ss.) (alterando a sua opinião inicial), Silveira; Freitas (2017, p. 57 e ss.), Coutinho (2014), Acórdão do TC n.º 382/2022 e Deliberações da CNPD n.ºs 641/2017 e 1008/2017, que consideravam/consideram que os Tribunais portugueses não podiam aplicar a Lei n.º 32/2008, por essa lei violar a CDFUE, ao passo que Gouveia (2014) e Ramos (2015, p. 127-128) (entendimento que veio a modificar posteriormente), não descartavam uma eventual proibição de aplicação.

IV A DECLARAÇÃO DE INCONSTITUCIONALIDADE COM FORÇA OBRIGATÓRIA GERAL DOS ARTIGOS 4.º, 6.º E 9.º (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) DA LEI N.º 32/2008, DE 17 DE JULHO

Como referimos, o Tribunal Constitucional, através do seu Acórdão n.º 268/2022, embora com um voto de vencido[23], declarou inconstitucionais, com força obrigatória geral, a norma constante do artigo 4.º da Lei n.º 32/2008, conjugada com o artigo 6.º da mesma Lei, por violação do disposto nos artigos 35.º, n.ºs 1 e 4, e 26.º, n.º 1, em conjugação com o artigo 18.º, n.º 2, todos da CRP, e a norma constante do artigo 9.º da Lei n.º 32/2008 (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 nos artigos 35.º, n.º 1, e 20.º, n.º 1, em conjugação com o artigo 18.º, n.º 2, todos da CRP.

Como também referimos, o aresto do TC foi prolatado no âmbito de um pedido de declaração de inconstitucionalidade dos artigos 4.º, 6.º e 9.º da Lei n.º 32/2008, em sede de fiscalização abstrata sucessiva à luz do artigo 281.º da CRP, formulado pela Provedora da Justiça, com fundamento na violação do Direito da União Europeia (artigos 7.º, 8.º e 52.º, n.º 1, da CDFUE, na sequência da declaração de invalidade da Diretiva 2006/24/CE pelo TJUE através do seu Acórdão de 8 de abril de 2014, *Digital Rights Ireland Ltd e Kärntner Landesregierung*), do direito à reserva da

[23] Cfr. Declaração de Voto do Cons. Lino José Batista Rodrigues Ribeiro, que subscrevemos em grande parte.

intimidade da vida privada e familiar (artigo 26.º, n.º 1, da CRP), do princípio da proporcionalidade (artigo 18.º, n.º 2, da CRP), do sigilo das comunicações (artigo 34.º da CRP) e do direito a uma tutela jurisdicional efetiva (artigo 20.º, n.º 1, da CRP), tendo o TC apreciado a constitucionalidade das referidas normas também à luz do direito à autodeterminação informacional, tutelado pelo artigo 35.º da CRP, e do direito ao livre desenvolvimento da personalidade, também tutelado pelo artigo 26.º, n.º 1, da CRP, pois considerou que o princípio do pedido não obsta a que o TC possa declarar a inconstitucionalidade das normas cuja apreciação foi requerida com fundamento diverso daqueles cuja violação foi invocada, invocando, para tal, o disposto no artigo 51.º, n.º 5, da LTC.

Cumpre, desde já, referir que o TC não declarou a inconstitucionalidade das referidas normas à luz do direito ao sigilo das comunicações[24].

Em síntese, o TC, apreciando separadamente a vertente da conservação (artigos 4.º e 6.º da Lei n.º 32/2008) – e, dentro dela, analisou primeiro os dados de base e depois os dados de tráfego e de localização, cuja conservação considerou mais intensamente restritiva de direitos fundamentais do que a conservação dos dados de base – da vertente da transmissão (artigo 9.º), baseou o juízo de inconstitucionalidade nos seguintes aspetos:

a) no que tange à conservação dos dados de base, ainda que a sua conservação tal como está regulada na Lei n.º 32/2008 não viole os ditames do princípio da proporcionalidade, o disposto no artigo 35.º, n.ºs 1 e 4, da CRP, interpretado em conformidade com os artigos 7.º e 8.º da CDFUE, impõe ao legislador, como condição de efetividade das garantias nele consagradas, a previsão da obrigatoriedade do armazenamento dos dados pessoais (como é o caso dos dados de base) num Estado-Membro da União Europeia e tal não é exigido pelos artigos 4.º e 6.º nem por qualquer outra norma da

[24] O que motivou uma declaração de voto dos Cons. Afonso Patrão, José João Abrantes, Assunção Raimundo e Mariana Canotilho.

Lei n.º 32/2008 ou de outro diploma vigente na ordem jurídica portuguesa;

b) no que tange à conservação dos dados de tráfego e de localização, mesmo quando não sejam gerados em virtude de uma comunicação pessoal, além de a lei não prever a obrigatoriedade do armazenamento dos dados pessoais num Estado-Membro da União Europeia, a sua conservação tal como está regulada na Lei n.º 32/2008 constitui uma restrição desproporcionada dos direitos à reserva da intimidade da vida privada e à autodeterminação informacional na medida em que são conservados todos os dados de localização e de tráfego de todos os assinantes, abrangendo as comunicações eletrónicas da quase totalidade da população, incluindo pessoas relativamente às quais não há qualquer suspeita de atividade criminosa, e sem qualquer diferenciação, exceção ou ponderação face ao objetivo visado;

c) no que tange à transmissão dos dados conservados, ainda que a sua conservação tal como está regulada na Lei n.º 32/2008 não viole os ditames do princípio da proporcionalidade, a lei não prevê a obrigatoriedade da notificação das pessoas cujos dados relativos às suas comunicações foram transmitidos às autoridades públicas a partir do momento em que tal comunicação não seja suscetível de comprometer as investigações nem a vida ou a integridade física de terceiros (ainda que essas pessoas, embora por sua iniciativa, possam indagar se existiu algum acesso aos seus dados), o que constitui uma restrição desproporcionada dos direitos ao acesso a uma tutela judicial efetiva e à autodeterminação informacional.

Como se disse, tal entendimento não foi unânime, porquanto foi lavrado um voto de vencido, cujos fundamentos subscrevemos

na sua maioria (e não na sua totalidade), embora considerando que poderão ser invocados outros argumentos adicionais e que o entendimento que foi acolhido pela maioria dos Juízes do TC é, ele próprio, inconstitucional. Inconstitucionalidade essa que não é afastada pelo facto de o Acórdão n.º 268/2022 acabar por funcionar como uma espécie de transposição de vários arestos do TJUE para a nossa ordem jurídica interna. Aliás, por essa razão, padece de vícios análogos aos de que os arestos do TJUE em causa padecem, embora à luz do Direito da União Europeia.

No entanto, iremos cingir a nossa análise ao Direito português, embora relembrando, desde já, que, nos termos do artigo 3.º, n.º 2, do Tratado da União Europeia (TUE), "a União proporciona aos seus cidadãos um espaço de liberdade, segurança e justiça sem fronteiras internas, em que seja assegurada a [...] prevenção da criminalidade e combate a este fenómeno"[25] e que a CDFUE também garante, no seu artigo 6.º, os direitos à liberdade e à segurança, bem como, noutros preceitos, diversos direitos fundamentais que constituem o substrato constitucional de bens jurídicos tutelados por diversos tipos de crime particularmente graves e cuja prevenção e repressão são essenciais num Estado de Direito, como, por exemplo, os direitos à vida (artigo 2.º), à integridade pessoal (artigo 3.º), a não ser escravizado nem alvo de redução à servidão ou sujeito a tráfico de seres humanos (artigo 5.º), à propriedade (artigo 17.º), à saúde (artigo 35.º), ao ambiente (artigo 37.º), a uma boa administração (artigo 41.º), à ação e a um Tribunal imparcial (artigo 47.º), *etc*., que, na nossa óptica, não foram tidos em conta (ou, pelo menos, não o foram na correta medida) pelo TJUE. E o mesmo sucede com os direitos ao respeito pela vida privada e familiar (artigo 7.º) e à proteção de dados pessoais (artigo 8.º), que também podem ser lesados por via da prática de crimes, pelo

[25] E, de acordo com o artigo 67.º, n.º 3, do TFUE, "a União envida esforços para garantir um elevado nível de segurança, através de medidas de prevenção da criminalidade, do racismo e da xenofobia e de combate contra estes fenómenos, através de medidas de coordenação e de cooperação entre autoridades policiais e judiciárias e outras autoridades competentes, bem como através do reconhecimento mútuo das decisões judiciais em matéria penal e, se necessário, através da aproximação das legislações penais.".

que não podem ser considerados apenas para justificar a limitação da utilização de medidas de investigação criminal.

Assim, passando a apresentar os nossos argumentos no sentido da inadequação do decidido pelo TC, em primeiro lugar, ao contrário do que é afirmado pelo TC (e aqui divergimos do voto de vencido) e pelo TJUE, a mera conservação de metadados não restringe qualquer direito fundamental, sendo que apenas ocorre uma restrição no momento em que eles sejam acedidos.

Na verdade, tal como exigem os artigos 3.º, n.º 3, e 7.º, n.º 2, da Lei n.º 32/2008, os metadados terão de ser guardados em ficheiros (*que têm de estar obrigatoriamente separados de quaisquer outros ficheiros para outros fins*) e *encriptados* e, nos termos dos artigos 3.º, n.ºs 1 e 2, 8.º e 9.º, n.º 1 (abstraindo do facto de, como referimos, considerarmos que este preceito foi tacitamente revogado pela Lei n.º 109/2009).

Esses ficheiros só podem ser desencriptados e acedidos para fins de investigação, deteção e repressão de crimes graves por parte das autoridades competentes e mediante despacho judicial fundamentado[26]. E, além disso, só os funcionários do operador de comunicações eletrónicas que estejam especialmente autorizados para tal poderão aceder aos dados, sob pena de responsabilidade penal[27] (e a sua identidade tem de ser comunicada à CNPD, sob pena de responsabilidade contraordenacional[28]). Ou seja, na fase de conservação, os metadados são, apenas e só, inseridos em ficheiros

[26] Atento o facto de entendermos que o artigo 9.º da Lei n.º 32/2008 foi revogado pelos artigos 12.º e ss. da Lei n.º 109/2009, a entidade competente para autorizar o acesso aos metadados é a autoridade judiciária no caso de dados de base e de localização celular (cfr. artigo 14.º, n.ºs 1 e 4, da Lei n.º 109/2009) e, no caso dos dados de tráfego, o JIC ou o Juiz (cfr. artigos 18.º, n.º 2, da Lei n.º 109/2009, na fase de inquérito, e 189.º, n.º 2, do CPP, nas demais fases processuais). Aliás, não vemos em que medida a obtenção de dados conservados terá de ser rodeada de maiores garantias do que no caso de esses dados serem obtidos em tempo real, razão pela qual entendemos ser desajustado sujeitar o acesso a dados de base ou de localização conservados a autorização judicial quando a obtenção desses dados em tempo real pode ser autorizada pelo MP na fase de inquérito.

[27] Cfr. artigo 13.º, n.º 1, alínea c), da Lei n.º 32/2008.

[28] Cfr. artigo 12.º, n.º 1, alínea d), da Lei n.º 32/2008.

que ficarão encriptados e intocados até à sua destruição ao fim de 1 ano, a menos que seja autorizado o acesso a determinados metadados (apenas os relativos ao arguido, ao suspeito, ao intermediário ou, mediante consentimento, à vítima e não a todos os metadados que estejam naquele ou naqueles ficheiros) e nada mais: a mera conservação, por si só, não revela quaisquer informações, apenas permitindo o uso futuro de elementos de prova em investigações criminais que, de outro modo, teriam desaparecido e não poderiam ser utilizados, sendo que, num Estado de Direito, esse aumento da eficácia da investigação só pode ser considerado positivamente[29].

[29] De facto, o Tribunal Europeu dos Direitos Humanos (TEDH) tem considerado que a proteção dos direitos fundamentais inclui o dever de as autoridades levarem a cabo uma investigação efetiva e eficaz (no sentido de serem utilizados meios de investigação que se mostrem necessários para investigar no caso concreto) em ordem a investigar os crimes que atinjam algum dos direitos fundamentais garantidos pela Convenção Europeia dos Direitos Humanos (CEDH), desde logo no caso de homicídios, tendo em conta o disposto no artigo 2.º da CEDH (cfr. Acórdãos McCann e Outros c. Reino Unido, Mahmut Kaya c. Turquia, Hugh Jordan c. Reino Unido, Paul e Audrey Edwards c. Reino Unido, Nachova e Outros c. Bulgária, Kaya e Outros c. Turquia, Ramsahai e Outros c. Países Baixos, Angelova e Iliev c. Bulgária, Opuz c. Turquia, Kolevi c. Bulgária, Al-Skeini e Outros c. Reino Unido, Vasîlka c. Moldávia, Jaloud c. Países Baixos, Mustafa Tunç e Fecire Tunç c. Turquia e Armani da Silva c. Reino Unido).
E, no que concerne à obtenção de metadados numa investigação criminal, o TEDH considerou que a não obtenção de metadados que se mostre necessária para uma determinada investigação criminal de crimes cometidos através da Internet ou com utilização da Internet (*v. g*., divulgação de vídeos anteriormente obtidos através de uma câmara oculta colocada no domicílio da vítima, permitindo a obtenção dos metadados identificar o autor da publicação e, eventualmente, o autor das gravações ilícitas) é incompatível com o artigo 8.º da CEDH (que também inclui um dever positivo de as autoridades levarem a cabo uma investigação efetiva e eficaz relativamente a crimes que lesem os direitos fundamentais tutelados por esse preceito da CEDH) se essa não obtenção puser em causa a eficácia dessa mesma investigação [cfr. Acórdãos K.U. c. Finlândia, Khadija Ismayilova c. Azerbaijão e Volodina c. Rússia (N.º 2)]. Aliás, no Acórdão K.U. c. Finlândia é particularmente evidente a censura do TEDH à excessiva importância que foi atribuída pelas autoridades finlandesas à confidencialidade dos dados de tráfego dos internautas face à necessidade de identificar o indivíduo que publicou um anúncio na Internet, desse modo tornando um menor em alvo de abordagens de pedófilos, sendo que a lei finlandesa em vigor, que visava proteger a liberdade de expressão e o direito à expressão anónima e protegia os autores de mensagens anónimas na Internet, impedia as autoridades de, numa tal situação, imporem ao fornecedor de serviços o fornecimento de metadados que permitissem a identificação do agente da infração, o que votara ao insucesso a investigação que fora aberta.

Daí que não se nos afigure razoável defender a existência de uma restrição de direitos fundamentais ao nível da mera conservação dos dados, assim como também não existe no caso da preservação expedita de dados informáticos e na revelação expedita de dados de tráfego previstas nos artigos 12.º e 13.º da Lei n.º 109/2009 (Cfr. NUNES, 2021a, p. 84 e 101). E, por isso, o disposto nos artigos 4.º e 6.º da Lei n.º 32/2008 jamais poderia ser inconstitucional.

Em segundo lugar, mesmo que se admitisse (que não admitimos) que a mera conservação de metadados restringe direitos fundamentais, tratar-se-ia, em todo e qualquer caso, de restrições muito pouco significativas. Assim, no caso dos dados de base, trata-se dos elementos necessários para o acesso à rede (*v. g.*, nome, data de nascimento, morada, estado civil, número de telefone, PIN, PUK, IMEI, IMSI, endereço eletrónico, IP[30]), sendo que o próprio TC acaba por considerar que se trata de uma restrição pouco intensa.

No caso dos dados de localização a que a Lei n.º 32/2008 se refere, a única informação que esses dados fornecem é a localização de um determinado dispositivo (que nem sequer permite determinar com toda a exatidão qual é esse local), a partir da qual se vai *inferir* (de forma ilidível) que o seu proprietário ou utilizador habitual se encontrava nesse mesmo local, sendo incorreto afirmar que os dados de localização permitem *saber* a localização de uma pessoa. Por isso, a obtenção (e não a conservação, que não revela quaisquer dados) de dados de localização celular constitui uma restrição muito pouco significativa de direitos fundamentais[31].

Acresce que a União Europeia aderiu à CEDH e, além disso, os direitos fundamentais tal como a CEDH os garante e tal como resultam das tradições constitucionais comuns aos Estados-Membros fazem parte do Direito da União Europeia enquanto princípios gerais, (cfr. artigo 6.º, n.ºs 2 e 3, do TUE).

[30] No que tange às diferenças de regime jurídico relativamente à obtenção do IP estático e do IP dinâmico, *vide* Nunes (2021a, p. 110-111).

[31] Cfr. Nunes (2019b, p. 133), Acórdãos do TC n.º 486/2009 e do Supremo Tribunal de Justiça (STJ) de 29/04/2010 e Sentenças do *Bundesgerichtshof* (BGH) de 24/01/2001 e do *Tribunal Supremo* n.º 6307/2009; contra, Acórdão do TC n.º 268/2022 e Sentença United States *v.* Jones do *Supreme Court of the United States*.

Por fim, no caso dos dados de tráfego, trata-se dos elementos ou dados funcionais necessários ou produzidos pelo estabelecimento da ligação através da qual uma comunicação concreta é operada ou transmitida [a direção, o destino (*adressage*) e a via, o trajeto (*routage*)], os quais se limitam a revelar – no caso de comunicações telefónicas – os números das chamadas recebidas e os números para os quais aquele dispositivo ligou (daí se *inferindo*, uma vez mais de forma ilidível, que as comunicações tiveram lugar entre os proprietários ou os utilizadores habituais de cada um desses números telefónicos) e a data, a duração, a hora, e a frequência dessas comunicações ou tentativas de comunicação e nada mais, pois nada revelam quanto ao conteúdo das comunicações.

Por isso, trata-se de uma restrição também pouco intensa de direitos fundamentais e que, por ser muito menos intensa do que no caso da obtenção de dados de conteúdo, a sua obtenção, ainda que restrinja o direito à inviolabilidade das comunicações, nem deveria estar sujeita ao regime particularmente restritivo das interceções de comunicações (cfr. NUNES, 2019a, p. 577), como sucede no Direito alemão (em que o legislador consagrou, no § 100g StPO[32], um regime muito menos restritivo do que o das interceções de comunicações do § 100a).

Em terceiro lugar, a conservação e os ulteriores acesso e utilização de metadados têm por finalidade exclusiva a investigação, deteção e repressão de crimes graves por parte das autoridades competentes (cfr. artigo 3.º, n.º 1, da Lei n.º 32/2008), o que inclui a repressão criminal e a prevenção criminal, tendo em conta o *continuum* que existe (e terá de existir[33]) entre ambas como *conditio sine qua non* para responder eficazmente à criminalidade organizada, ao terrorismo, à criminalidade económico-financeira e ao cibercrime (cfr. NUNES, 2019a, p. 581). Como referimos, os metadados são conservados em ficheiros separados dos demais ficheiros e ficam encriptados e intocados até à sua destruição ao fim de um ano, a menos que seja autorizado o acesso a metadados relativos ao

[32] *Strafprozessordnung*.
[33] Sobre esse *continuum*, *vide* Nunes (2019a, p. 255 e ss.).

arguido, ao suspeito, ao intermediário ou, mediante consentimento, à vítima (e não a todos os metadados que estejam naquele ou naqueles ficheiros).

Além disso, se atentarmos no catálogo do artigo 2.º, n.º 1, alínea g), da Lei n.º 32/2008[34], estão em causa crimes gravíssimos, como, por exemplo, crimes de homicídio doloso, ofensa à integridade física grave, mutilação genital feminina, ofensa à integridade física agravada pelo resultado, violência doméstica, violação, coação sexual, abuso sexual de menores, roubo, extorsão, associação criminosa, tráfico de órgãos humanos, tráfico de pessoas, tráfico de armas, tráfico de estupefacientes, corrupção, tráfico de influência, participação económica em negócio, branqueamento de capitais, organizações terroristas, terrorismo, financiamento do terrorismo, rapto, sequestro agravado, tomada de reféns, escravidão, tortura e outros tratamentos cruéis, degradantes e desumanos, crimes contra a segurança do Estado ou contrafação de moeda.

E, como sabemos, para que a criminalização de uma conduta seja admissível, terá de estar em causa a proteção de um bem jurídico essencial à convivência comunitária e ao livre desenvolvimento da pessoa, que terá de estar relacionado com um direito fundamental ou com um interesse constitucionalmente protegido, sendo os bens jurídico-penais concretizações dos valores constitucionais expressa ou implicitamente ligados aos direitos e deveres fundamentais e à ordenação social, política e económica (cfr. DIAS, 2019, p. 136 e ss.; NUNES, 2021b, p. 84). Deste modo, no caso dos crimes que referimos, está em causa a proteção de alguns dos bens mais relevantes à luz da ordem de valores jurídico-constitucional.

Ora, a utilização de metadados tende a ser absolutamente essencial para muitas investigações criminais desses tipos de crime

[34] Embora consideremos que a obtenção de dados de localização ou de base não está sujeita a qualquer catálogo de crimes (cfr. artigo 14.º da Lei n.º 109/2009) e que a obtenção de dados de tráfego está sujeita (*de jure condito*) ao catálogo do artigo 18.º, n.º 1, da Lei n.º 109/2009, que é mais amplo do que o catálogo do artigo 2.º, n.º 1, alínea g), da Lei n.º 32/2008.

(e de outros)[35], *maxime* quando se trate de formas de criminalidade que utilizam sistematicamente meios informáticos e/ou outros meios eletrónicos de comunicação à distância (designadamente, a criminalidade organizada, o terrorismo[36], a criminalidade económico-financeira, ou o cibercrime[37] *ex se*) cuja utilização gere metadados.

E, como é óbvio, a notícia do crime é sempre obtida após a prática do crime (e, não poucas vezes, muito depois), já para não falar dos casos em que, mesmo que o processo seja instaurado pouco tempo após a prática do crime, a identificação de arguidos ou suspeitos só ocorre muito tempo depois da instauração do processo (e só aí, salvo no caso da vítima, é que a obtenção de metadados relativos ao suspeito, ao arguido ou ao intermediário será possível e admissível). Por isso, os metadados que se interessa obter são metadados gerados no passado e não no decurso da investigação[38], sendo essa situação que o legislador pretendeu acautelar ao impor a

[35] Não poucas vezes, para lograrem identificar os agentes do crime, as autoridades têm necessariamente de determinar quais eram os telemóveis/cartões que acionaram um conjunto de células/antenas de telecomunicações no lapso de tempo em que os factos terão sido praticados (estando, muitas vezes, em causa um lapso de tempo de apenas alguns minutos) e a identidade dos respetivos proprietários (a fim de inferir quem eram as pessoas que se encontravam naquele local para, numa segunda fase, conseguir identificar os autores do crime), sendo que é frequente estarem em causa crimes extremamente graves (homicídios, raptos, roubos, assaltos a caixas multibanco com utilização de explosivos, *etc*.) (*vide*, a este respeito, NUNES, 2019b, *passim*).

[36] Aliás, é sabido que as investigações criminais dos atentados terroristas de Madrid (11/03/2004) e Londres (07/07/2005) foram bem-sucedidas graças à reconstituição das comunicações eletrónicas entre os vários intervenientes das redes terroristas em causa, pois foi essa reconstituição que permitiu às autoridades perceberem as relações existentes entre eles.

[37] Que, quando entendido em sentido lato (tal como defendemos), inclui tanto os crimes em que o sistema informático ou os dados informáticos são o objeto da ação, ainda que como alvos simbólicos (cibercrime em sentido estrito) como outros crimes cujo cometimento esteja significativamente ligado à utilização de um sistema informático (onde se incluem, por exemplo, a pornografia infantil, a extorsão sexual, o tráfico de drogas ou armas, o jogo ilícito *online*, as burlas relativas a criptomoedas, etc.) (cfr. NUNES, 2021a, p. 45-46).

[38] Cuja obtenção, em regra, apenas tem interesse no caso de atividades criminosas duradouras em que, no decurso da investigação, vão sendo cometidos novos crimes ou novos atos do crime sob investigação (*v. g.*, no caso dos crimes de tráfico ou de abuso sexual de menores).

conservação dos metadados através da Lei n.º 32/2008 e o mesmo sucedendo com o Parlamento Europeu e o Conselho ao adotarem a Diretiva 2006/24/CE.

Tendo em conta o que acabámos de referir, além de a mera conservação de metadados não restringir direitos fundamentais (e, ainda que restringisse, tratar-se-ia de uma restrição pouco intensa) e de o acesso aos metadados constituir uma restrição pouco intensa de direitos fundamentais, a desconsideração (ao ponto de ocorrer um sacrifício a 100% do valor da segurança[39] e também dos demais direitos fundamentais que se concretizam nos bens jurídico-penais tutelados pelos crimes constantes do catálogo do artigo 2.º, n.º 1, alínea g), da Lei n.º 32/2008 quando acaba por impedir a conservação e o acesso a esses dados nos termos dos artigos 4.º, 6.º e 9.º dessa lei) da necessidade de responder eficazmente aos crimes graves constantes do catálogo do artigo 2.º, n.º 1, alínea g), da Lei n.º 32/2008 configura uma proteção insuficiente dos direitos fundamentais que se concretizam nos bens jurídico-penais tutelados por esses crimes[40]. E é certo que a Lei n.º 32/2008 encontrou um equilíbrio que proporciona uma muito adequada concordância prática entre os bens e valores em jogo[41].

Aliás, atentas à natureza dos crimes que integram o catálogo do artigo 2.º, n.º 1, alínea g), da Lei n.º 32/2008, à intensidade da restrição de direitos fundamentais que o acesso aos metadados acarreta[42] e às salvaguardas que o legislador previu na lei, os direitos ou interesses constitucionalmente protegidos prosseguidos através da investigação criminal tendem a ser mais relevantes à luz da ordem de valores jurídico-constitucional do que os direitos fundamentais restringidos, o que foi completamente invertido pelo TC. E não podemos olvidar que o interesse público numa Justiça penal funcionalmente eficaz é um pressuposto essencial do Estado

[39] Cfr. Voto de vencido do Acórdão do TC n.º 268/2022.
[40] Como resulta da jurisprudência do TEDH que referimos.
[41] Como se aduz no Voto de vencido do Acórdão do TC n.º 268/2022.
[42] Sendo que, no caso da conservação, não ocorre qualquer restrição e, a ocorrer, seria pouco intensa e inclusivamente menos intensa do que no caso do acesso.

de Direito e possui, também ele, respaldo constitucional[43], sendo que a investigação dos crimes e a punição dos criminosos é levada a cabo em prol do interesse da Comunidade no seu todo e não em prol do engrandecimento do Estado.

Em quarto lugar, como se afirma no voto de vencido, se só for possível conservar metadados (designadamente no caso de dados de tráfego e de localização) relativamente a pessoas em relação às quais existam indícios de que o seu comportamento possa ter algum *nexo* com os crimes graves enunciados na alínea g) do n.º 1 do artigo 2.º da Lei n.º 32/2008, os fornecedores de serviços de telecomunicações apenas podem conservar os dados quando a autoridade judiciária competente os solicitar no decurso de uma investigação criminal, situação que já está prevista no artigo 12.º da Lei n.º 109/2009, de 15 de setembro[44] (mas cuja aplicação depende de os dados a preservar terem sido previamente conservados)[45], mas não se mostra eficaz para garantir a recolha de prova em processo penal. Isto porque, por exemplo, numa situação de rapto, se os dados relativos às comunicações das vítimas forem apagados findas que sejam tais comunicações, poderá ser muito difícil identificar os agentes dos crimes, sendo os metadados que viessem a ser obtidos em tempo real tendencialmente inúteis.

[43] Cfr. Dias (2011, p. 37 e ss.), Nunes (2019a, p. 335 e ss.), Correia (2014, p. 39, nota 21), Acórdãos Paul e Audrey Edwards c. Reino Unido do TEDH, do TC n.º 213/2008, do STJ de 03/03/2010 e do TRL de 24/01/2012 e Sentenças do *Bundesverfassungsgericht* (BVerfG) de 27/06/2018, National City Trading Corp. *v.* United States do *United States Court of Appeals, 2nd Circuit* (1980) e United States *v.* Hunter do *United States District Court, Vermont* (1998).

[44] O texto integral da Lei n.º 109/2009, de 15 de setembro (lei do Cibercrime) está disponível no endereço <*https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1137&tabela=leis*>.

[45] Aliás, em consequência da decisão do TC – e caso não seja possível encontrar um caminho alternativo no Direito vigente no que tange às normas julgadas inconstitucionais (e sem prejuízo de considerarmos que o artigo 9.º da Lei n.º 32/2008 fora já revogado pelos artigos 12.º e ss. da Lei n.º 109/2009 –, os artigos 12.º (na parte em que estejam em causa dados de tráfego, de base e/ou de localização), 13.º e 14.º, n.º 4, da Lei n.º 109/2009 ficaram temporariamente esvaziados de conteúdo, só voltando a ter aplicabilidade prática quando entrar em vigor uma nova lei relativa à conservação de metadados (já que no que tange ao acesso, os meios de obtenção de prova previstos na Lei n.º 109/2009 são perfeitamente adequados para esse fim).

No fundo, uma tal exigência é impossível de observar no caso da conservação de metadados a que se refere a Lei n.º 32/2008, que, como vimos, é um instrumento absolutamente essencial para muitas investigações criminais, *maxime* quando se trate de formas de criminalidade de dificílima investigação e que utilizam sistematicamente meios informáticos e/ou outros meios eletrónicos de comunicação à distância (designadamente, a criminalidade organizada, o terrorismo, a criminalidade económico-financeira ou o cibercrime *ex se*) cuja utilização gere metadados.

Na verdade, a conservação de metadados a que se refere a Lei n.º 32/2008 é uma medida de prevenção criminal que se integra na chamada investigação proativa (que é essencial para responder às novas formas de criminalidade, em que uma investigação meramente reativa, *i. e.*, apenas a partir da obtenção da notícia do crime, é manifestamente ineficaz), sendo que a investigação proativa inicia-se num momento prévio à prática do crime ou ao conhecimento da sua prática pelas autoridades e visa, entre outras finalidades, obter uma *notitia criminis*, obter informações que facilitem a investigação de crimes que venham a ser cometidos (como sucede no caso da conservação de metadados ou da imposição de deveres de colaboração/reporte ao abrigo da Lei n.º 83/2017, de 18 de agosto) ou relativas ao modo de funcionamento de certas formas de criminalidade (as chamadas informações de *intelligence*) ou evitar o cometimento de crimes já planeados ou minimizar os seus efeitos para as vítimas (cfr. NUNES, 2019a, p. 256-257).

Dito de outro modo, num momento prévio à obtenção da notícia do crime é *impossível* indicar qualquer critério delimitador dos metadados a conservar. E, ainda que fosse possível, tal critério sempre violaria os princípios da proibição da discriminação (como veremos infra) e da presunção de inocência. No fundo, o TC formulou uma exigência que é de observância impossível e que contradiz a natureza preventiva, proativa da conservação de metadados e, com isso, declarou a inconstitucionalidade dos artigos 4.º e 6.º da Lei n.º 32/2008, negando, na prática – salvo se for possível encontrar vias alternativas no Direito vigente – a possibilidade de utilização de

metadados na investigação criminal, que é um meio absolutamente necessário para responder às mais graves formas de criminalidade da atualidade.

Em quinto lugar, como se afirma no voto de vencido, na medida em que o artigo 35.º, n.ºs 1 e 4, da CRP autoriza a informatização de dados pessoais sem o consentimento do titular e remete para a lei a definição dessas condições, não se pode aferir a observância dos ditames do princípio da proporcionalidade separando o regime da conservação dos dados pelos operadores de telecomunicações do regime de acesso aos mesmos. Na verdade, como aí se refere, a redação originária do artigo 35.º, n.º 1, apenas ressalvava o "disposto na lei sobre segredo de Estado e segredo de justiça", mas, na revisão de 1997 adotou-se uma fórmula mais ampla ("nos termos da lei"), para possibilitar outras restrições ao direito de acesso, designadamente no caso de medidas necessárias em matéria de segurança do Estado, defesa, segurança pública, prevenção, investigação, detenção e repressão de infrações penais, restrições que já estavam previstas no artigo 13.º da Diretiva 95/46/CE do Parlamento Europeu e do Conselho. Ora, a Lei n.º 32/2008 é um dos diplomas para os quais o artigo 35.º, n.º 4, da CRP remete a previsão de exceções à proibição de acesso a dados pessoais de terceiros, sendo que, se apenas as autoridades judiciárias tiverem acesso aos dados encriptados, com base em pressupostos previamente definidos, é óbvio que as oportunidades de devassa e difusão dos dados pessoais são escassas.

Em sexto lugar, apesar de a Lei n.º 32/2008 ser o diploma através do qual o legislador transpôs a Diretiva 2006/24/CE para o Direito português, a declaração de invalidade da Diretiva não implica por si só a invalidade da Lei n.º 32/2008 à luz do Direito União Europeia, pois a conservação e obtenção de registos da realização de comunicações e de dados de localização não depende, *ex se*, dessa Diretiva, nada impedindo a sua consagração legal na falta de uma tal Diretiva (cfr. NUNES, 2019a, p. 559). Ademais, o legislador nacional criou um quadro normativo que vai muito para além da Diretiva ao prever um regime jurídico que cumpre as exigências cuja inobservância pela Diretiva que levaram o TJUE a declarar a

invalidade da Diretiva não sejam aplicáveis à Lei n.º 32/2008[46].

Em sétimo lugar, como se refere no voto de vencido, a lei permite que os operadores conservem, pelo prazo de seis meses, uma grande parte dos metadados incluídos no artigo 4.º da Lei n.º 32/2008 para efeitos de faturação (cfr. artigos 6.º, n.º 3, e 7.º da Lei 41/2004, de 18 de agosto, e 9.º, n.º 2 e 10.º. n.º 1, da Lei n.º 23/96 de 26 de julho), sem que isso ponha em causa a privacidade dos utilizadores, ao ponto de não ter sido também peticionada a declaração da inconstitucionalidade das normas que permitem a conservação para efeitos de faturação.

Ora, não se pode conceber que o interesse privado das operadoras cobrarem os serviços prestados aos seus clientes possa ser mais relevante do que o interesse público numa Justiça penal funcionalmente eficaz, sobretudo quando se trate da investigação de crimes que atentam contra os valores mais eminentes da ordem de valores jurídico-constitucional (como sucede com a vida e/ou a integridade pessoal, que a CRP reputa expressamente como invioláveis) e exista o perigo de criminosos que cometeram crimes graves e foram punidos por sentença transitada em julgado virem a ser absolvidos na sequência de um recurso de revisão procedente e da consequente reelaboração da Sentença com expurgo das provas obtidas através de metadados, ao ponto de se admitir como constitucionalmente admissível a conservação de dados para efeitos de faturação e o mesmo já não suceder no caso de conservação para fins de investigação criminal.

Em oitavo lugar, como também se refere no voto de vencido, o TJUE considerou que a conservação de dados só é admissível quando obedeça a três critérios objetivos (um período temporal, uma zona geográfica determinada e um círculo determinado de pessoas), sendo que uma medida legislativa de conservação preventiva de dados, geograficamente condicionada, dirigida a um círculo de pessoas determinadas e sem qualquer facto típico cometido não

[46] Relativamente às razões por que entendemos que os fundamentos que levaram o TJUE a declarar a invalidade da Diretiva não são aplicáveis à Lei n.º 32/2008, *vide* Nunes (2019a, p. 559 e ss.).

é tolerada pela norma do n.º 3 do artigo 35.º da CRP, que apenas admite que o legislador autorize tratamento informático de dados relativos à vida privada "*com garantias de não discriminação*". Por isso, o entendimento do TJUE, além de lhe serem assacáveis *mutatis mutandis* as críticas que formulamos ao entendimento do TC, viola o princípio da igualdade e a proibição de discriminação (e também a presunção de inocência), pelo que, ao acolher o entendimento do TJUE, o TC também viola o princípio da igualdade e a proibição de discriminação e a presunção de inocência (pois está a suspeitar-se de que aquele concreto visado poderá ter cometido ou vir a cometer crimes de que nem sequer existe notícia), o que configura uma primeira causa da inconstitucionalidade do entendimento perfilhado pelo TC no Acórdão n.º 268/2022.

Em nono lugar, no que diz respeito à não previsão da obrigatoriedade de que os dados estejam armazenados num Estado-Membro da União Europeia, como se aduz no voto de vencido, é um problema que nem sequer se deveria colocar, pois o artigo 7.º, n.º 4, da Lei n.º 32/2008 remete para as Leis n.ºs 67/98, de 26 de outubro (sendo que, atualmente, a questão está regulada nos arts. 44.º e ss. do RGPD), e 41/2004, de 18 de agosto, onde se resolve a questão da territorialidade e da transferência dentro e para fora da União Europeia (o que torna desnecessária a repetição dessa regulação na Lei n.º 32/2008). E, além disso, quando a lei sujeita a conservação dos dados ao controlo da CNPD, está a impor, implicitamente, que os dados terão de estar armazenados no território português.

Em décimo lugar, em sentido contrário dos demais argumentos que já esgrimimos e esgrimiremos de seguida, as provas que os metadados podem proporcionar tanto podem servir para provar a prática de crimes pelo arguido como para este demonstrar a sua inocência ou, no mínimo, fazer surgir no julgador uma dúvida razoável, pelo que também a defesa (e não apenas a acusação) fica impossibilitada de utilizar tais provas, com as quais poderia impedir condenações insustentável e materialmente injustas.

Em décimo primeiro lugar, no que diz respeito à não notificação dos titulares dos dados de que os seus dados foram acedidos pelas

autoridades, desde logo, na maioria das situações, essa notificação sempre seria completamente desnecessária e redundante, dado que, na maioria das investigações, os dados que foram acedidos são os dados do ou dos arguidos, que, tendo acesso aos autos, terão perfeito conhecimento de que os seus dados foram acedidos e poderão exercer os seus direitos a esse respeito. Além disso, como se refere no voto de vencido, o artigo 9.º da Lei n.º 32/2008 nem sequer é a sede para regular se e quando o titular dos dados deve ser notificado pelas autoridades judiciárias do acesso e transmissão de dado, pelo que declarar a inconstitucionalidade deste preceito com um tal fundamento não faz qualquer sentido. Ademais, é manifestamente excessivo e desrazoável declarar a inconstitucionalidade de uma norma e, com isso, vedar o recurso a um meio de obtenção de prova absolutamente essencial para investigar crimes graves, com um tal fundamento, sobretudo tendo em conta as consequências jurídicas que poderão advir de uma tal decisão.

Em décimo segundo lugar, se atentarmos nas consequências jurídicas expectáveis de uma tal declaração de inconstitucionalidade, o decidido pelo TC, no caso de não ser possível encontrar vias alternativas aos artigos 4.º, 6.º e 9.º da Lei n.º 32/2008 no Direito vigente para obter metadados para as investigações criminais pode abrir a porta a consequências absolutamente devastadoras em termos de resposta à criminalidade (e, como tal, de proteção dos direitos fundamentais dos cidadãos, pois a prática de crimes também constitui um atentado contra os direitos fundamentais dos cidadãos em geral e das vítimas em particular), de restabelecimento da paz jurídica e de realização da justiça penal e de credibilidade da Justiça e do próprio Estado de Direito. Assim, no que tange aos processos em curso, não poderão ser obtidos metadados e os que tiverem sido obtidos não poderão ser usados como prova (o que pode comprometer de sobremaneira a eficácia das investigações e conduzir a decisões absolutórias[47] insustentável e materialmente injustas, bem como, na medida em que também a defesa fica impossibilitada de os usar, conduzir a decisões condenatórias insustentável e materialmente

[47] Nas "decisões absolutórias" devemos incluir, além de sentenças absolutórias, os despachos de arquivamento e os despachos de não pronúncia.

injustas ou, pelo menos, à sujeição do arguido a julgamento de forma absolutamente desnecessária).

Mas a situação poderá ser ainda mais dramática no que tange a condenações transitadas em julgado (sobretudo no caso de crimes graves, de criminosos perigosos e/ou de condenações em penas de prisão efetiva), em que, por força do disposto no artigo 449.º, n.º 1, alíneas e) ou f), do CPP[48], nos casos em que os metadados tenham sido decisivos para a condenação (*maxime* quando tenha sido através dos metadados que foi possível dirigir a investigação e obter as provas que sustentaram a condenação – que dificilmente teria sido possível descobrir sem a prévia obtenção dos metadados – ou quando, no caso de condenações com base em prova indiciária, tenham sido os metadados que permitiram retirar dos indícios a prova dos factos constitutivos do crime[49]), indivíduos que comprovadamente cometeram crimes (e, por isso, foram condenados) acabarem por ser absolvidos, com tudo o que isso possa acarretar em termos de prevenção geral e especial, para as vítimas do crime (que poderão vir a ser confrontadas com a absolvição de criminosos que haviam efetivamente cometido crimes contra si e que haviam sido condenados com trânsito em julgado) e, em última análise, para a credibilidade da Justiça e do Estado de Direito aos olhos dos cidadãos. E mesmo no caso do arguido, as provas que os metadados podem proporcionar também podem servir para o arguido demonstrar a sua inocência ou, no mínimo, fazer surgir no julgador uma dúvida razoável.

[48] No entanto, as condenações transitadas em julgado só poderão ser postas em causa por via da interposição de um recurso extraordinário de revisão, que terá de ser julgado procedente pelo STJ, para que, então, a sentença possa ser reelaborada, sendo expurgada das provas obtidas através de metadados conservados à luz da Lei n.º 32/2008, embora sem prejuízo de essas provas serem mantidas (e a condenação mantida nos seus precisos termos) no caso de se concluir que poderiam ter sido obtidas por outra via que não os artigos 4.º, 6.º e 9.º da Lei n.º 32/2008.

[49] Será muito pouco provável que alguma condenação se baseie exclusivamente em metadados, mas as situações referidas no texto são altamente plausíveis. Na verdade, os metadados podem ter sido a prova que permitiu chegar a todas as outras e, por isso, a todas contaminar com o seu efeito à distância.

E é por força de tudo isto que haverá que convocar um último argumento (que também constitui um fundamento para afirmar que o entendimento perfilhado pelo TC é inconstitucional) e que tem a ver com o próprio princípio da proporcionalidade. De facto, o princípio da proporcionalidade não possui apenas uma vertente de proibição do excesso (*Übermaßverbot*), possuindo igualmente uma vertente de proibição de insuficiência (*Untermaßverbot*), que é violada quando as entidades (designadamente, o Estado em todas as suas funções: legislativa, jurisdicional e administrativa) oneradas com um dever de proteção (*Schutzpflicht*) não adotam medidas ou adotam medidas insuficientes para garantir uma proteção constitucionalmente adequada dos direitos fundamentais[50]. Aí se incluindo, por exemplo, a adoção de medidas inadequadas ou ineficazes, o não aperfeiçoamento das medidas existentes, a adoção de medidas que desprotejam os cidadãos face às ameaças ou agressões provenientes de outros cidadãos e a "anulação" de medidas existentes de que resulte uma proteção insuficiente de direitos fundamentais (cfr. ISENSEE, 1983, p. 40; BALTAZAR JÚNIOR, 2010, p. 68; NUNES, 2019a, p. 322; HAIN, 1993, p. 983; UNRUH, 1996, p. 24-25; PIETRZAK, 1994, p. 750 e 752-753). E a proibição de insuficiência vale também no plano do Direito Penal (e Processual Penal)[51], sendo que, como bem afirma Isensee (2000, p. 218), o cumprimento do dever estatal de proteção da segurança dos cidadãos tanto poderá consistir na adoção de medidas repressivas como de medidas preventivas.

É evidente que a proibição de insuficiência não pode ser radicalizada, sob pena de ultrapassagem dos limites de facto e direito a que o legislador está adstrito numa Sociedade livre e democrática (cfr. ANDRADE, 2004, p. 149; ISENSEE, 2000, p. 155; NUNES, 2019a, p. 325), mas também não pode ser desvalorizada ao ponto de

[50] Assim, Canotilho (2002, p. 273), segundo o qual, ocorre um defeito de proteção (e, como tal, uma violação *Untermassverbot*) "quando as entidades sobre quem recai um dever de proteção (*Schutzpflicht*) adotam medidas insuficientes para garantir uma proteção constitucionalmente adequada dos direitos fundamentais".

[51] Acerca dos corolários do princípio da proporcionalidade na vertente de proibição de insuficiência e dos deveres estatais de proteção ao nível do Direito penal (em sentido amplo), *vide* Nunes (2019a, p. 330 e ss.), com vastas referências doutrinárias e jurisprudenciais.

a esvaziar ou quase esvaziar de efeito útil em favor da proibição do excesso, jamais se podendo afirmar que a proibição de insuficiência apenas vale na medida do possível[52].

A proibição de insuficiência corresponde ao patamar mínimo de proteção do direito fundamental, ao passo que a proibição do excesso corresponde ao patamar máximo admissível da restrição, vigorando a liberdade de conformação do legislador (que define o "*como*" da proteção dos direitos fundamentais dos cidadãos face a ameaças ou a agressões provenientes de terceiros) no espaço que medeia entre o patamar mínimo de proteção e o limite máximo da restrição (neste sentido, NUNES, 2019a, p. 328.).

Na medida em que, no momento da aplicação ao caso concreto, ambas as vertentes do princípio da proporcionalidade poderão colidir entre si, haverá que compatibilizá-las, encontrando a proibição de insuficiência limites na proibição do excesso e vice-versa, pois a violação da proibição de insuficiência também pode resultar de uma incorreta aplicação da proibição do excesso e vice-versa (assim, NUNES, 2019a, p. 328-329).

E, na nossa óptica, como referimos, o entendimento perfilhado no Acórdão do TC n.º 268/2022 é ele próprio inconstitucional, porquanto dele resulta uma proteção insuficiente dos direitos fundamentais que se concretizam nos bens jurídico-penais tutelados pelos crimes constantes do catálogo do artigo 2.º, n.º 1, alínea g), da Lei n.º 32/2008 ao impossibilitar a conservação e o acesso a esses dados nos termos dos artigos 4.º, 6.º e 9.º dessa lei quando:

a) a mera conservação de metadados, sobretudo tendo em conta o modo com eles são armazenados nos termos da lei, não restringe qualquer direito fundamental;

b) ainda que o acesso aos metadados restringisse direitos fundamentais, fá-lo-ia sempre de uma forma pouco intensa (pelas razões sobreditas), jamais justificando a proteção desses direitos fundamentais (para mais quando

[52] Como faz Andrade (2004, p. 149) [sobre a nossa crítica a esta afirmação, *vide* Nunes (2019a, p. 330 (nota 1269)].

são alvo de uma restrição pouco intensa) a completa desconsideração das necessidades de resposta eficaz aos crimes graves constantes do catálogo do artigo 2.º, n.º 1, alínea g), da Lei n.º 32/2008, como sucede no aresto em análise;

c) assenta numa exigência impossível de cumprir em face da natureza preventiva da conservação de metadados (no momento em que os dados são conservados não existe nem poderá existir qualquer suspeita e não é possível definir qualquer critério no que tange à seleção de pessoas cujos dados podem ser conservados sem se violar os princípios da proibição da discriminação e da presunção de inocência) cujo (inevitável) incumprimento é utilizado como fundamento para declarar a inconstitucionalidade;

d) é manifestamente excessivo declarar a inconstitucionalidade de uma norma e, com isso, vedar o recurso a um meio de obtenção de prova absolutamente essencial para investigar crimes graves (e para o arguido demonstrar a sua inocência ou, no mínimo, fazer surgir no julgador uma dúvida razoável), apenas porque essa norma não prevê a obrigatoriedade da notificação dos titulares dos dados de que os seus dados foram acedidos pelas autoridades quando, pela sua natureza, não caberia a essa norma regular uma tal matéria e, na maioria das situações, essa notificação sempre seria completamente desnecessária e redundante, dado que, na maioria das investigações, os dados que foram acedidos são os dos arguidos, que, tendo acesso aos autos, terão perfeito conhecimento de que os seus dados foram acedidos e poderão exercer os seus direitos a esse respeito; e

e) irá dificultar de sobremaneira a resposta à criminalidade grave (*maxime* a criminalidade organizada, o terrorismo, a criminalidade económico-financeira, a criminalidade violenta, a criminalidade sexual e o cibercrime) ao impedir – caso não seja possível encontrar no Direito

> vigente uma via alternativa – a conservação preventiva dos metadados e o acesso a ele ou a valoração das provas já obtidas no âmbito dos processos em curso e, no caso de condenações transitadas em julgado, poderá abrir a porta a insustentáveis situações de impunidade com a absolvição de criminosos que haviam sido condenados por Sentenças transitadas em julgado no caso de o recurso de revisão interposto ser julgado procedente e de os factos criminosos não poderem ser dados como provados sem a valoração dos metadados.

Contudo, apesar de tudo o que acabámos de referir, a declaração de inconstitucionalidade dos artigos 4.º, 6.º e 9.º da Lei n.º 32/2008 (que retirou todo e qualquer efeito útil a essa lei) é irreversível, apenas restando procurar uma via alternativa (caso exista) no Direito vigente que permita evitar os efeitos nefastos – e existindo o risco de serem devastadores – que recenseámos supra, servindo o que temos vindo a referir para reforçar a premência da procura de uma tal solução. Ademais, as provas que os metadados podem proporcionar tanto podem servir para provar a prática de crimes pelo arguido como para este demonstrar a sua inocência ou, no mínimo, fazer surgir no julgador uma dúvida razoável, pelo que também a defesa (e não apenas a acusação) fica impossibilitada de utilizar tais provas.

V A ADMISSIBILIDADE DA UTILIZAÇÃO DE METADADOS NA INVESTIGAÇÃO CRIMINAL APESAR DA DECLARAÇÃO DE INCONSTITUCIONALIDADE POR VIA DO ACÓRDÃO DO TRIBUNAL CONSTITUCIONAL N.º 268/2022

Pese embora a declaração de inconstitucionalidade dos artigos 4.º, 6.º e 9.º da Lei n.º 32/2008, como acabámos de referir, torna-se imperativo, desde logo para obstar à violação do princípio da proibição de insuficiência por via do défice de proteção dos

direitos fundamentais que se concretizam nos bens jurídico-penais tutelados pelos crimes constantes do catálogo do artigo 2.º, n.º 1, alínea g), da Lei n.º 32/2008 e condenações do Estado português no TEDH (por força dos deveres positivos de levar a cabo investigações criminais relativamente a crimes que lesem direitos fundamentais garantidos pela CEDH que o TEDH tem considerado recaírem sobre as autoridades), procurar caminhos alternativos no nosso Direito vigente.

Caso logremos encontrar um ou mais caminhos alternativos, além de continuar a ser admissível obter metadados e valorar as provas proporcionadas pelos metadados anteriormente obtidos nos processos em curso, a eventual lesão do artigo 126.º do CPP[53] que poderia fundamentar um recurso de revisão no caso das condenações transitadas em julgado não terá ocorrido, pois os dados poderiam ter sido legitimamente obtidos com base em normas diversas dos artigos 4.º, 6.º e 9.º da Lei n.º 32/2008 agora declaradas inconstitucionais.

A tarefa mais fácil, até tendo em conta aquele que sempre foi o nosso entendimento no que tange às relações entre a Lei n.º 32/2008 e a Lei n.º 109/2009, é a que se refere à determinação da norma que permite o acesso e a consequente obtenção dos metadados conservados para o processo.

E, a nosso ver, as normas que permitem obter os metadados conservados para o processo são o artigo 14.º, n.º 4, da Lei n.º 109/2009 (no caso dos dados de base e de localização) e, no caso dos dados de tráfego, os artigos 18.º, n.º 2, da Lei n.º 109/2009 (na fase de inquérito) e 189.º, n.º 2, do CPP (nas demais fases processuais), continuando a ser possível lançar mão do disposto no artigo 12.º da Lei n.º 109/2009 (no que tange à preservação expedita dos dados, que consiste na emissão de uma ordem a quem tenha a disponibilidade ou

[53] Embora entendamos que a conservação de metadados não restringe direitos fundamentais, o TC considerou o contrário, o que não pode deixar de relevar na hora de aferir se se verifica, ou não, o fundamento do recurso de revisão previsto no artigo 449.º, n.º 1, alínea e), do CPP. Diversamente, no caso do acesso e obtenção de metadados já ocorre uma restrição (ainda que pouco intensa) de direitos fundamentais previstos no artigo 126.º, n.º 3, do CPP.

o controlo de quaisquer dados informáticos específicos armazenados num sistema informático que adote as medidas necessárias para proteger esses dados de tudo o que possa alterar ou deteriorar a sua qualidade ou o seu estado atual. Ainda assim, mantendo-os a salvo de toda e qualquer modificação, danificação ou eliminação, a fim de não comprometer a produção de prova) (cfr. NUNES, 2021a, p. 76-77).

É certo que o TC – embora de uma forma completamente desproporcionada e desrazoável – considerou que o artigo 9.º da Lei n.º 32/2008 é inconstitucional em virtude de não estar prevista a obrigatoriedade da 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. Todavia, tal poderá ser colmatado por via de, apesar de a lei o não prever, a autoridade judiciária notificar as pessoas cujos metadados tenham sido acedidos logo que essa notificação não seja suscetível de comprometer as investigações (quer a investigação naquele processo quer noutros processos) nem a vida, integridade física ou a liberdade (incluindo a liberdade e a autodeterminação sexual) de terceiros, assim se afastando este argumento na eventualidade de um recurso para o TC em sede de fiscalização concreta.

Deste modo, as autoridades podem legitimamente aceder, para fins de investigação criminal, a metadados previamente conservados pelos operadores de comunicações eletrónicas[54].

[54] Mesmo anteriormente à entrada em vigor da Lei n.º 109/2009, dado que antes desse momento (e da entrada em vigor da Lei n.º 32/2008) já vigoravam o artigo 189.º, n.º 2 (ao abrigo do qual era possível obter dados de tráfego e de localização celular, não distinguindo a lei se se tratava de dados obtidos em tempo real ou de dados conservados, sendo que a Lei n.º 41/2004 já então vigorava) e os artigos 125.º e 135.º (à luz dos quais era possível obter os dados de base), ambos do CPP. Ademais, antes da entrada em vigor da Lei n.º 32/2008 e da reforma de 2007 do CPP, a jurisprudência admitia a obtenção de dados de tráfego (que já então eram conservados à luz da Lei n.º 41/2004) junto dos operadores de comunicações eletrónicas [cfr., entre outros, Acórdãos do TRC de 17/05/2006 e 15/11/2006, do Tribunal da Relação de Guimarães (TRG) de 10/01/2005 e 21/11/2005 e do TRE de 26/06/2007].

No entanto, para que esse acesso (e ulterior valoração) possa ter lugar, os metadados terão de ter sido conservados e, mais do que isso, legitimamente conservados.

E, no que tange à prévia conservação de metadados (ainda que não para efeitos de investigação criminal), nos termos dos artigos 6.º, n.º 3, e 7.º da Lei n.º 41/2004, de 18 de agosto, e 9.º, n.º 2 e 10.º. n.º 1, da Lei n.º 23/96 de 26 de julho[55], os operadores de comunicações eletrónicas poderão conservar os metadados por seis meses (que é o período durante o qual a fatura pode ser legalmente contestada ou o pagamento reclamado), sendo que, se essa conservação é legalmente admissível para efeitos de salvaguarda de direitos privados dos operadores de comunicações eletrónicas de cariz patrimonial (cobrança dos serviços prestados), por maioria de razão, é igualmente legítimo o acesso das autoridades a tais dados (legitimamente conservados) para fins de investigação criminal, prosseguindo-se, dessa forma, o interesse público numa Justiça penal funcionalmente eficaz (que é um pressuposto essencial do Estado de Direito e possui, também ele, respaldo constitucional), sendo que a investigação dos crimes e a punição dos criminosos é levada a cabo em prol do interesse da Comunidade no seu todo e não em prol do engrandecimento do Estado nem de interesses meramente privados. De notar que não nos parece que o decidido pelo TC no Acórdão n.º 268/2022 impeça os operadores de fornecerem às autoridades os dados que conservam nos termos da Lei n.º 41/2004.

No entanto, contra este nosso entendimento poderão ser aduzidos vários argumentos, embora todos estejam condenados ao naufrágio.

Assim, em primeiro lugar, poderá aduzir-se que o entendimento que defendemos passa (não na fase de conservação, mas sim na fase de transmissão) por uma "alienação do fim" ("*Zweckentfremdung*"), pois, ao serem subsequentemente acedidos e valorados num processo penal, os metadados irão ser utilizados para uma finalidade

[55] O texto integral da Lei n.º 23/96, de 26 de julho, está disponível no endereço <*https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1436&tabela=leis*>.

diversa daquela para a qual foram conservados. E, de facto, é isso que acontece. Contudo, pese embora o que resulta do Acórdão n.º 268/2022 do TC, o direito à autodeterminação informacional (de que a proibição de "alienação do fim" é um instrumento de tutela) não é absoluto e, além disso, como referimos, a mera conservação de metadados não restringe quaisquer direitos fundamentais (sendo que é a própria Lei n.º 41/2004 que "informa" os utilizadores de comunicações eletrónicas de que os seus metadados podem ser conservados pelos fornecedores de tais serviços) e o ulterior acesso a tais dados restringe direitos fundamentais de uma forma pouco intensa. E estando em causa a resposta à criminalidade grave, a "alienação do fim" jamais poderá constituir um óbice à obtenção e valoração de metadados para fins de investigação criminal, sob pena de violação da proibição de insuficiência.

E, em segundo lugar, poderá aduzir-se que o TJUE[56] entendeu que o artigo 15.º, n.º 1, da Diretiva 2002/58/CE (que foi transposta para o Direito português por via da Lei n.º 41/2004), conforme alterada pela Diretiva 2009/136/CE, lido à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da CDFUE, deve ser interpretado no sentido de que se opõe a uma regulamentação nacional que preveja, para

[56] Cfr. Acórdãos de 21 de dezembro de 2016, *Tele2 Sverige AB e Secretary of State for the Home Department*, de 6 de outubro de 2020, *Privacy International*, de 6 de outubro de 2020, *La Quadrature du Net e Outros* (que, no entanto, admite a conservação generalizada e indiferenciada dos endereços IP atribuídos à fonte de uma ligação por um período temporalmente limitado ao estritamente necessário e dos dados relativos à identidade civil dos utilizadores de meios de comunicações eletrónicos, o que continua a ser manifestamente insuficiente), de 2 de março de 2021, *Prokuratuur*, e de 5 de abril de 2022, *G.D.* (que decidiu, ainda, que o Direito da União deve ser interpretado no sentido de que se opõe a que um órgão jurisdicional nacional limite no tempo os efeitos de uma declaração de invalidade que lhe incumbe, por força do direito nacional, relativamente a uma legislação nacional que impõe aos prestadores de serviços de comunicações eletrónicas uma conservação generalizada e indiferenciada dos dados de tráfego e dos dados de localização, em razão da incompatibilidade dessa legislação com o artigo 15.º, n.º 1, da Diretiva 2002/58, conforme alterada pela Diretiva 2009/136, lido à luz da Carta dos Direitos Fundamentais, bem como que a admissibilidade dos meios de prova obtidos através dessa conservação cabe, em conformidade com o princípio da autonomia processual dos Estados-Membros, ao Direito nacional, sob reserva do respeito, nomeadamente, dos princípios da equivalência e da efetividade).

efeitos de luta contra a criminalidade, uma conservação generalizada e indiferenciada de todos os dados de tráfego e dados de localização de todos os assinantes e utilizadores registados em relação a todos os meios de comunicação eletrónica, bem como a uma regulamentação nacional que regule a proteção e a segurança dos dados de tráfego e dos dados de localização, em especial, o acesso das autoridades nacionais competentes aos dados conservados, sem limitar, no âmbito da luta contra a criminalidade, esse acesso apenas para efeitos de luta contra a criminalidade grave, sem submeter o referido acesso a um controlo prévio por parte de um órgão jurisdicional ou de uma autoridade administrativa independente, e sem exigir que os dados em causa sejam conservados em território da União Europeia. No entanto, os dados conservados nos termos da Lei n.º 41/2004 não se destinam à investigação criminal (como sucedia no caso da Diretiva 2006/24/CE e da Lei n.º 32/2008), pelo que – sem prejuízo de entendermos que os arestos do TJUE sofrem, *mutatis mutandis*, dos mesmos vícios que apontámos ao Acórdão do TC n.º 268/2022 – a jurisprudência do TJUE não impede a conservação de metadados para as finalidades previstas na Lei n.º 41/2004 nem os ulteriores acesso e valoração dos mesmos para efeitos de investigação criminal.

Em suma, apesar do decidido pelo TC no seu Acórdão n.º 268/2022, as autoridades poderão aceder, para fins de investigação criminal, aos metadados conservados à luz da Lei n.º 41/2004 e obtê-los para o processo (e valorá-los) com base no artigo 14.º, n.º 4, da Lei n.º 109/2009 (no caso dos dados de base e de localização) e, no caso dos dados de tráfego, nos artigos 18.º, n.º 2, da Lei n.º 109/2009 (na fase de inquérito) e 189.º, n.º 2, do CPP (nas demais fases processuais).

E, a nosso ver, as normas que permitem obter os metadados conservados para o processo são o artigo 14.º, n.º 4, da Lei n.º 109/2009 (no caso dos dados de base e de localização) e, no caso dos dados de tráfego, os artigos 18.º, n.º 2, da Lei n.º 109/2009 (na fase de inquérito) e 189.º, n.º 2, do CPP (nas demais fases processuais), continuando a ser possível lançar mão do disposto no artigo 12.º da

Lei n.º 109/2009 no que tange à preservação expedita dos dados. E, desta forma, obtendo-se uma concordância prática adequada entre os direitos fundamentais em colisão, obsta-se aos efeitos nefastos que a impossibilidade de acesso, obtenção e valoração de metadados para fins de investigação criminal poderia ter nos processos em curso e, sobretudo, nas condenações transitadas em julgado que referimos supra.

E, como referimos, as provas que os metadados podem proporcionar tanto podem servir para provar a prática de crimes pelo arguido como para este demonstrar a sua inocência ou, no mínimo, fazer surgir no julgador uma dúvida razoável.

VI CONCLUSÕES

a) A Lei n.º 32/2008, de 17 de junho transpôs para a nossa ordem jurídica a Diretiva 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de março, 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 (metadados);

b) a conservação e a transmissão dos metadados têm por finalidade exclusiva a investigação, deteção e repressão de crimes graves por parte das autoridades competentes, sendo obrigatória a separação dos ficheiros destinados à conservação de dados de quaisquer outros ficheiros para outros fins e não podendo o titular dos dados opor-se à respetiva conservação e transmissão;

c) por força dos artigos 4.º a 6.º da Lei n.º 32/2008, os fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações estavam obrigados a, durante o período de um ano, conservar (1) os dados necessários para encontrar e identificar a fonte de uma comunicação, (2) os dados

necessários para encontrar e identificar o destino de uma comunicação, (3) os dados necessários para identificar a data, a hora e a duração de uma comunicação, (4) os dados necessários para identificar o tipo de comunicação, (5) os dados necessários para identificar o equipamento de telecomunicações dos utilizadores, ou o que se considera ser o seu equipamento e (6) os dados necessários para identificar a localização do equipamento de comunicação móvel, incluindo os dados telefónicos e da Internet relativos a chamadas telefónicas falhadas quando gerados, tratados e/ou armazenados por esses mesmos fornecedores de serviços de comunicações eletrónicas, mas não os dados relativos a chamadas não estabelecidas;

d) à exceção dos dados relativos ao nome e endereço dos assinantes, os demais metadados tinham de permanecer bloqueados (*i. e.*, encriptados) desde o início da sua conservação e, nos termos do artigo 9.º da Lei n.º 32/2008, só podiam ser desbloqueados (*i. e.*, desencriptados) para efeitos de transmissão às autoridades competentes, que, nos termos do artigo 2.º, n.º 1, alínea f), são as autoridades judiciárias (Juiz, JIC e MP) e as autoridades de polícia criminal, desde que se tratasse de metadados relativos ao arguido, ao suspeito, a pessoa relativamente à qual houvesse fundadas razões para crer que recebe ou transmite mensagens destinadas ou provenientes de suspeito ou de arguido ou à vítima de crime (neste último caso, mediante o respetivo consentimento);

e) o Juiz só poderia autorizar o acesso aos metadados se houvesse razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter no âmbito da investigação, deteção e repressão de crimes graves, que, nos termos do artigo 2.º, n.º 1, alínea g), são os crimes de terrorismo, criminalidade violenta,

criminalidade altamente organizada, sequestro, rapto e tomada de reféns, crimes contra a identidade cultural e integridade pessoal, contra a segurança do Estado, falsificação de moeda ou de títulos equiparados a moeda, contrafação de cartões ou outros dispositivos de pagamento, uso de cartões ou outros dispositivos de pagamento contrafeitos, aquisição de cartões ou outros dispositivos de pagamento contrafeitos, atos preparatórios da contrafação e crimes abrangidos por convenção sobre segurança da navegação aérea ou marítima, devendo a decisão judicial 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 proteção do segredo profissional.

f) a transmissão dos dados processava-se mediante comunicação eletrónica, nos termos das condições técnicas e de segurança fixadas na Portaria n.º 469/2009, que deviam observar um grau de codificação e proteção o mais elevado possível, de acordo com o estado da técnica ao momento da transmissão, incluindo métodos de codificação, encriptação ou outros adequados;

g) só os trabalhadores dos operadores de comunicações eletrónicas que estivessem especialmente autorizados para tal é que poderiam aceder aos metadados para os transmitir às autoridades, devendo cada operador manter junto da CNPD um registo eletrónico permanentemente atualizado desses trabalhadores;

h) o incumprimento de qualquer das regras relativas à proteção e à segurança dos metadados (incluindo a sua não encriptação) e o acesso aos dados por pessoa não especialmente autorizada constituem crime e o não envio à CNPD dos dados necessários à identificação das pessoas especialmente autorizadas constitui uma contraordenação;

i) o artigo 9.º da Lei n.º 32/2008 fora já tacitamente revogado pelos artigos 12.º e ss. da Lei n.º 109/2009, de 15 de setembro;

j) na sequência de o TJUE, em 2014, ter declarado a Diretiva 2006/24/CE inválida e apesar das garantias previstas na Lei n.º 32/2008 (que não padecia dos vícios que haviam levado o TJUE a declarar a invalidade da Diretiva), o TC, embora com um voto de vencido, veio agora declarar inconstitucionais, com força obrigatória geral, a norma constante do artigo 4.º da Lei n.º 32/2008, conjugada com o artigo 6.º da mesma lei, por violação do disposto nos artigos 35.º, n.ºs 1 e 4, e 26.º, n.º 1, em conjugação com o artigo 18.º, n.º 2, todos da CRP, e a norma constante do artigo 9.º da Lei n.º 32/2008 (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 nos artigos 35.º, n.º 1, e 20.º, n.º 1, em conjugação com o artigo 18.º, n.º 2, todos da CRP;

k) além de diversos outros aspetos em que o entendimento maioritário dos Juízes do TC é passível da censura que formulámos supra, tal entendimento padece, ele próprio, de inconstitucionalidade, por violação do disposto no artigo 35.º, n.º 3, da CRP e por violação do princípio da proporcionalidade na vertente de proibição de insuficiência ao – em face da absoluta necessidade da conservação e da utilização dos metadados para responder a muita da criminalidade da atualidade – conduzir a uma proteção manifestamente insuficiente dos direitos fundamentais em que se concretizam os bens jurídicos protegidos pelos crimes para cuja investigação a lei previa a utilização

dos metadados conservados (por exemplo, os crimes de homicídio doloso, ofensa à integridade física grave, mutilação genital feminina, ofensa à integridade física agravada pelo resultado, violência doméstica, violação, coação sexual, abuso sexual de menores, roubo, extorsão, associação criminosa, tráfico de órgãos humanos, tráfico de pessoas, tráfico de armas, tráfico de estupefacientes, corrupção, tráfico de influência, participação económica em negócio, branqueamento de capitais, organizações terroristas, terrorismo, financiamento do terrorismo, rapto, sequestro agravado, tomada de reféns, escravidão, tortura e outros tratamentos cruéis, degradantes e desumanos, crimes contra a segurança do Estado, *etc*.);

l) a declaração da inconstitucionalidade das referidas normas irá dificultar de sobremaneira a resposta à criminalidade grave (*maxime* a criminalidade organizada, o terrorismo, a criminalidade económico-financeira, a criminalidade violenta, a criminalidade sexual e o cibercrime) ao impedir – caso não seja possível encontrar no Direito vigente uma via alternativa – a conservação preventiva dos metadados e o acesso aos mesmos ou a valoração das provas já obtidas no âmbito dos processos em curso e, no caso de condenações transitadas em julgado, poderá abrir a porta a insustentáveis situações de impunidade por via da absolvição de criminosos (inclusivamente os que cometeram crimes graves como, por exemplo, homicídios) que haviam sido condenados por sentença transitada em julgado no caso de o recurso de revisão interposto ser julgado procedente e de os factos criminosos não poderem ser dados como provados sem a valoração dos metadados;

m) a lei vigente permite evitar as consequências nefastas referidas nas duas conclusões anteriores, dado que o artigo 14.º, n.º 4, da Lei n.º 109/2009 (no caso dos

dados de base e de localização) e, no caso dos dados de tráfego, os artigos 18.º, n.º 2, da Lei n.º 109/2009 (na fase de inquérito) e 189.º, n.º 2, do CPP (nas demais fases processuais) permitem obter dados de base, bem como os dados de tráfego e/ou de localização que tenham sido conservados pelos operadores de comunicações eletrónicas ao abrigo dos artigos 6.º, n.º 3, e 7.º da Lei n.º 41/2004, ainda que essa conservação se destinasse à cobrança dos serviços prestados aos clientes;

n) todavia, a solução que propomos é uma solução provisória e exige uma intervenção legislativa tão rápida quanto possível.

REFERÊNCIAS

ANDRADE, José Carlos Vieira de. **Os direitos fundamentais na constituição portuguesa de 1976**. 3. ed. Coimbra: Almedina, 2004.

ALEMANHA. Bundesgerichtshof. Sentença de 24 de janeiro de 2001. In: **Entscheidungen des Bundesgerichtshofes in Strafsachen**, Colónia e Berlim, Ed. Carl Heymanns, v. 46, p. 266 e ss., 2002.

ALEMANHA. Bundesverfassungsgericht. Sentença de 27 de junho de 2018 (2 BvR 1405/17; 2 BvR 1780/17). Disponível em: <https://www.bundesverfassungsgericht.de>. Consultado em: 14 jul. 2020.

BALTAZAR JÚNIOR, José Paulo. **Crime organizado e proibição de insuficiência**. Porto Alegre: Livraria do Advogado, 2010.

BASES de metadados das operadoras sem fiscalização há cinco anos. In: Diário de Notícias, de 15 maio 2022. Disponível em: <https://www.dn.pt/sociedade/bases-de-metadados-das-operadoras-sem-fiscalizacao-ha-cinco-anos14856834.html?fbclid=IwAR3MgNQHx4HpnD3KBAJiwqF1n9uIi233yFO8oAkJAr_E1XBc5qCEwCB6UC0>. Consultado em: 16

maio 2022.

CABREIRO, Carlos. Entrevista. In: Polícia viola leis ao investigar comunicações. Diário de Notícias, Lisboa, 7 de junho de 2014. Disponível em: <www.mynetpress.com/pdf/2014/junho/201406073814e7.pdf>. Consultado em: 2 dez. 2014.

CANOTILHO, José Joaquim Gomes. **Direito constitucional e teoria da constituição**. 5. ed. Coimbra: Almedina, 2002.

COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS. Deliberação n.º 641/2017. Disponível em: <www.cnpd.pt>.

COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS. Deliberação n.º 1008/2017. Disponível em: <www.cnpd.pt>.

COUTINHO, Francisco Pereira. Entrevista. In: Polícia viola leis ao investigar comunicações. Diário de Notícias, Lisboa, 7 de junho de 2014. Disponível em: <www.mynetpress.com/pdf/2014/junho/201406073814e7.pdf>. Consultado em: 2 dez. 2014.

CORREIA, João Conde. Prova digital: as leis que temos e a lei que devíamos ter. In: **Revista do Ministério Público**, Lisboa, Ed. Sindicato dos Magistrados do Ministério Público, n.º 139, p. 29 e ss., 2014.

DIAS, Jorge de Figueiredo. **Direito penal**: parte geral: questões fundamentais: a doutrina geral do crime. t. I. 3. ed. Coimbra: Coimbra Ed., 2019.

DIAS, Jorge de Figueiredo. **Acordos sobre a sentença em processo penal, o "fim" do estado de direito ou um novo "princípio"?** Porto: Conselho Distrital do Porto da Ordem dos Advogados, 2011.

ESPANHA. Tribunal Supremo. Sentença n.º 6307/2009. Disponível em: <www.poderjudicial.es>.

ESTADOS UNIDOS. Supreme Court of the United States.

Sentença United States v. Jones. Disponível em: <http://supreme.justia.com>. Consultado em: 05 mar. 2013.

ESTADOS UNIDOS. United States Court for the District of Vermont. Sentença United States v. Hunter, 13 F. Supp. 2d 574 (1998). Disponível em: <https://law.justia.com/cases/federal/district-courts/FSupp2/13/574/2311683/>. Consultado em: 14 jul. 2020.

ESTADOS UNIDOS. United States Court of Appeals. Sentença National City Trading Corp. v. United States, 635 F.2d 1020 (2nd Circuit, 1980). Disponível em: <https://casetext.com/case/national-city-trading-corp-v-united-states-2>. Consultado em: 14 jul. 2020.

GOUVEIA, Jorge Barcelar. Entrevista. In: Polícia viola leis ao investigar comunicações. Diário de Notícias, Lisboa, 7 de junho de 2014. Disponível em: <www.mynetpress.com/pdf/2014/junho/201406073814e7.pdf>. Consultado em: 2 dez. 2014.

HAIN, Karl-Eberhard. Der gesetzgeber in der klemme zwischen übermass - und untermassverbot. In: **Deutsches Verwaltungsblatt**, Colónia, Berlim, Bona, Munique, Ed. Carl Heymanns, ano 108, fascículo 18, p. 982 e ss., 1993.

ISENSEE, Josef. **Das grundrecht auf sicherheit, zu den schutzpflichten des freiheitlichen verfassungsstaates**. Berlim e Nova Iorque: Walter de Gruyter, 1983.

ISENSEE, Josef. § 111: das grundrecht als abwehrrecht und als staatliche schutzpflicht. In: ISENSEE, Josef; KIRCHHOF, Paul (Hg.). **Handbuch des staatsrechts der Bundesrepublik Deutschland**: allgemeine grundrechtslehren. v. V. 2. ed. Heidelberg: Müller Juristischer, 2000. p. 143 e ss.

MARTINS, A. G. Lourenço. Novas tecnologias, investigação criminal e o cidadão em vias de transparência. In: **Estudos em homenagem ao Prof. Doutor Manuel da Costa Andrade**. v. II. Coimbra: Ed. Universidade de Coimbra, Instituto Jurídico, 2017. p. 491 e ss.

MESQUITA, Paulo Dá. **Processo penal, prova e sistema**

judiciário. Coimbra: Coimbra Ed., 2010.

MILHEIRO, Tiago Caiado. Artigo 189.º. In: **Comentário judiciário do código de processo penal**: artigos 124º a 190º. t. II. Coimbra: Almedina, 2019.

NUNES, Duarte Rodrigues. **Curso de direito penal**: parte geral: questões fundamentais, teoria geral do crime. t. I. Coimbra: Gestlegal, 2021b.

NUNES, Duarte Rodrigues. Da admissibilidade da obtenção de dados de localização celular ou de dados de tráfego de todos os telemóveis/cartões que acionaram um determinado conjunto de antenas/células de telecomunicações no lapso de tempo em que o crime sob investigação terá sido praticado, para posterior identificação dos seus autores. In: **Revista do Ministério Público**, Lisboa, Ed. Sindicato dos Magistrados do Ministério Público, n.º 157, p. 125 e ss., 2019b.

NUNES, Duarte Rodrigues. **O problema da admissibilidade dos métodos "ocultos" de investigação criminal como instrumento de resposta à criminalidade organizada**. Coimbra: Gestlegal, 2019a.

NUNES, Duarte Rodrigues. **Os meios de obtenção de prova previstos na lei do cibercrime**. 2. ed. Coimbra: Gestlegal, 2021a.

PIETRZAK, Alexandra. Die schutzpflicht im verfassungsrechtlichen kontext: überblick und neue aspekte. In: **Juristische Schulung**, Munique e Frankfurt, Ed. Verlag Beck, p. 748 e ss., 1994.

PINHO, Carlos. Lei de retenção de dados de comunicações eletrónicas: aposentar ou reformar? In: **Revista do Ministério Público**, Lisboa, Ed. Sindicato dos Magistrados do Ministério Público, n.º 154, p. 167 e ss., 2018.

PORTUGAL. Supremo Tribunal de Justiça. Acórdão de 3 de março de 2010 (Processo 886/07.8PSLSB.L1.S1). Disponível em: <www.dgsi.pt>.

PORTUGAL. Supremo Tribunal de Justiça. Acórdão de 29 de abril de 2010 (Processo 128/05.0JDLSB-A.S1). Disponível em: <www.dgsi.pt>.

PORTUGAL. Tribunal Constitucional. Acórdão n.º 213/2008. Disponível em: <www.tribunalconstitucional.pt>.

PORTUGAL. Tribunal Constitucional. Acórdão n.º 268/2022. Disponível em: <www.tribunalconstitucional.pt>.

PORTUGAL. Tribunal Constitucional. Acórdão n.º 382/2022. Disponível em: <www.tribunalconstitucional.pt>.

PORTUGAL. Tribunal Constitucional. Acórdão n.º 420/2017. Disponível em: <www.tribunalconstitucional.pt>.

PORTUGAL. Tribunal Constitucional. Acórdão n.º 486/2009. Disponível em: <www.tribunalconstitucional.pt>.

PORTUGAL. Tribunal da Relação de Coimbra. Acórdão de 15 de novembro de 2006 (Processo 915/06.2TAAVR-A.C1) . Disponível em: <www.dgsi.pt>.

PORTUGAL. Tribunal da Relação de Coimbra. Acórdão de 17 de maio de 2006 (Processo 1265/06). Disponível em: <www.dgsi.pt>.

PORTUGAL. Tribunal da Relação de Coimbra. Acórdão de 26 de fevereiro de 2014 (Processo 559/12.0GBOBR-A.C1). Disponível em: <www.dgsi.pt>.

PORTUGAL. Tribunal da Relação de Évora. Acórdão de 6 de janeiro de 2015 (Processo 6793/11.6TDLSB-A.E1). Disponível em: <www.dgsi.pt>.

PORTUGAL. Tribunal da Relação de Évora. Acórdão de 26 de junho de 2007 (Processo 843/07-1). Disponível em: <www.dgsi.pt>.

PORTUGAL. Tribunal da Relação de Évora. Acórdão de 22 de

fevereiro de 2022 (Processo 188/21.7GAVNO.E1). Disponível em: <www.dgsi.pt>.

PORTUGAL. Tribunal da Relação de Guimarães. Acórdão de 10 de janeiro de 2005 (Processo 2013/04-1). Disponível em: <www.dgsi.pt>.

PORTUGAL. Tribunal da Relação de Guimarães. Acórdão de 21 de novembro de 2005 (Processo 1987/05-1). Disponível em: <www.dgsi.pt>.

PORTUGAL. Tribunal da Relação de Lisboa. Acórdão de 22 de janeiro de 2013 (Processo 581/12.6PLSNT-A.L1-5). Disponível em: <www.dgsi.pt>.

PORTUGAL. Tribunal da Relação de Lisboa. Acórdão de 24 de janeiro de 2012 (Processo 35/07.2PJAMD.L1-5). Disponível em: <www.dgsi.pt>.

PORTUGAL. Tribunal da Relação de Lisboa. Acórdão de 28 de novembro de 2018 (Processo 8617/17.8T9LSB-A.L1-3). Disponível em: <www.dgsi.pt>.

RAMALHO, David Silva; COIMBRA, José Duarte. A declaração de invalidade da Diretiva 2006/24/CE: presente e futuro da regulação sobre conservação de dados de tráfego para fins de investigação, deteção e repressão de crimes graves. In: **O Direito**, Lisboa, Ed. Almedina, ano 147.º, p. 997 e ss., 2015.

RAMOS, Armando Dias. A prova digital na investigação do (ciber) terrorismo. In: **Investigação Criminal**, Lisboa, ASFIC, n.º 9, p. 111 e ss., 2015.

RAMOS, Armando Dias. **O agente encoberto digital**. Coimbra: Almedina, 2022.

SILVEIRA, Alessandra; FREITAS, Pedro Miguel. Implicações da declaração de invalidade da Diretiva 2006/24 na conservação de dados ("metadados") nos estados-membros da UE: uma

leitura jusfundamental. In: **Revista de Direito, Estado e Telecomunicações**, Brasília, Ed. UnB, v. 9, n.º 1, p. 47 e ss., 2017.

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA/TRIBUNAL DE JUSTIÇA DA COMUNIDADE EUROPEIA. Acórdão de 2 de março de 2021, Prokuratuur, Processo C-746/18. Disponível em: <http://curia.europa.eu>.

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA/TRIBUNAL DE JUSTIÇA DA COMUNIDADE EUROPEIA. Acórdão de 5 de abril de 2022, G.D., Processo C-140/20. Disponível em: <http://curia.europa.eu>.

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA/TRIBUNAL DE JUSTIÇA DA COMUNIDADE EUROPEIA. Acórdão de 6 de outubro de 2020, La Quadrature du Net e Outros, Processos C-511/18, C-512/18 e C-520/18. Disponível em: <http://curia.europa.eu>.

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA/TRIBUNAL DE JUSTIÇA DA COMUNIDADE EUROPEIA. Acórdão de 6 de outubro de 2020, Privacy International, Processo C-623/17. Disponível em: <http://curia.europa.eu>.

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA/TRIBUNAL DE JUSTIÇA DA COMUNIDADE EUROPEIA. Acórdão de 21 de dezembro de 2016, Tele2 Sverige AB e Secretary of State for the Home Department, Processos C-203/15 e C-698/15. Disponível em: <http://curia.europa.eu>.

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA/TRIBUNAL DE JUSTIÇA DA COMUNIDADE EUROPEIA. Acórdão Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources e Outros e Kärntner Landesregierung e Outros (de 8 de abril de 2014, Processos C-293/12 e C-594/12). Disponível em: <http://curia.europa.eu>.

TRIBUNAL EUROPEU DOS DIREITOS HUMANOS. Acórdão Al-Skeini e Outros c. Reino Unido (de 7 de julho de 2011). Disponível em: <https://hudoc.echr.coe.int/>.

TRIBUNAL EUROPEU DOS DIREITOS HUMANOS. Acórdão Angelova e Iliev c. Bulgária (de 26 de julho de 2007). Disponível em: <https://hudoc.echr.coe.int/>.

TRIBUNAL EUROPEU DOS DIREITOS HUMANOS. Acórdão Armani da Silva c. Reino Unido (30 de março de 2016). Disponível em: <https://hudoc.echr.coe.int/>.

TRIBUNAL EUROPEU DOS DIREITOS HUMANOS. Acórdão Hugh Jordan c. Reino Unido (de 4 de maio de 2001). Disponível em: <https://hudoc.echr.coe.int/>.

TRIBUNAL EUROPEU DOS DIREITOS HUMANOS. Jaloud c. Países Baixos (de 20 de novembro de 2014). Disponível em: <https://hudoc.echr.coe.int/>.

TRIBUNAL EUROPEU DOS DIREITOS HUMANOS. Acórdão Kaya e Outros c. Turquia (de 24 de outubro de 2006). Disponível em: <https://hudoc.echr.coe.int/>.

TRIBUNAL EUROPEU DOS DIREITOS HUMANOS. Acórdão Khadija Ismayilova c. Azerbaijão (10 de janeiro de 2019). Disponível em: <https://hudoc.echr.coe.int/>.

TRIBUNAL EUROPEU DOS DIREITOS HUMANOS. Acórdão Kolevi c. Bulgária (de 5 de novembro de 2009). Disponível em: <https://hudoc.echr.coe.int/>.

TRIBUNAL EUROPEU DOS DIREITOS HUMANOS. Acórdão K.U. c. Finlândia (de 2 de dezembro de 2008). Disponível em: <https://hudoc.echr.coe.int/>.

TRIBUNAL EUROPEU DOS DIREITOS HUMANOS. Acórdão McCann e Outros c. Reino Unido (de 27 de setembro de 1995). Disponível em: <https://hudoc.echr.coe.int/>.

TRIBUNAL EUROPEU DOS DIREITOS HUMANOS. Acórdão Mahmut Kaya c. Turquia (de 28 de março de 2000). Disponível em: <https://hudoc.echr.coe.int/>.

TRIBUNAL EUROPEU DOS DIREITOS HUMANOS. Acórdão Mustafa Tunç e Fecire Tunç c. Turquia (de 14 de abril de 2015). Disponível em: <https://hudoc.echr.coe.int/>.

TRIBUNAL EUROPEU DOS DIREITOS HUMANOS. Acórdão Nachova e Outros c. Bulgária (de 6 de julho de 2005). Disponível em: <https://hudoc.echr.coe.int/>.

TRIBUNAL EUROPEU DOS DIREITOS HUMANOS. Acórdão Opuz c. Turquia (de 9 de junho de 2009). Disponível em: <https://hudoc.echr.coe.int/>.

TRIBUNAL EUROPEU DOS DIREITOS HUMANOS. Acórdão Paul e Audrey Edwards c. Reino Unido (de 14 de março de 2002). Disponível em: <https://hudoc.echr.coe.int/>.

TRIBUNAL EUROPEU DOS DIREITOS HUMANOS. Acórdão Ramsahai e Outros c. Países Baixos (de 15 de maio de 2007). Disponível em: <https://hudoc.echr.coe.int/>.

TRIBUNAL EUROPEU DOS DIREITOS HUMANOS. Acórdão Vasîlka c. Moldávia (de 11 de fevereiro de 2014). Disponível em: <https://hudoc.echr.coe.int/>.

TRIBUNAL EUROPEU DOS DIREITOS HUMANOS. Acórdão Volodina c. Rússia (n.º 2) (de 14 de setembro de 2021). Disponível em: <https://hudoc.echr.coe.int/>.

UNRUH, Peter. Z**ur dogmatik der grundrechtlichen schutzpflichten**. Berlim: Duncker & Humblot, 1996.

Recebido em: 3-5-2023
Aprovado em: 2-7-2023