Revista Jurídica vol. 01, n°. 73, Curitiba, 2023. pp. 145 - 158

RETENÇÃO E UTILIZAÇÃO DE METADADOS DE COMUNICAÇÕES ELECTRÓNICAS: REFLEXÕES A PROPÓSITO DO ACÓRDÃO DO TRIBUNAL CONSTITUCIONAL N.º 268/2022, DE 3 DE JUNHO

RETENTION AND USE OF ELECTRONIC COMMUNICATIONS METADATA: BRIEF REFLECTIONS ON THE CONSTITUTIONAL COURT JUDGMENT NO. 268/2022, OF JUNE 3RD

CARLOS GABRIEL DA SILVA LOUREIRO

Licenciado e Mestre em Direito pela Faculdade de Direito da Universidade de Coimbra (Portugal). Doutorando em Direito na Universidade do Minho (Portugal); Professor-Adjunto na Escola Superior de Gestão do Instituto Politécnico do Cávado e do Ave (Portugal); Advogado. E-mail: cgloureiro@ipca.pt.

MAGDA CERQUEIRA

Juíza de direito no Tribunal da Comarca de Braga (Portugal); Licenciada em Direito pela Faculdade de Direito da Universidade de Coimbra; Mestre em Direito pela Universidade do Minho (Portugal). Doutoranda em Direito Judiciário na Universidade do Minho (Portugal). E-mail: magda851@gmail.com.

RESUMO

Objectivos: O presente visa proceder à análise das dificuldades suscitadas pelos metadados de comunicações electrónicas enquanto instrumento de investigação criminal, partindo do recente Acórdão do Tribunal Constitucional português n.º 268/2022, de 3 de Junho.

Metodologia: Procede-se ao estudo analítico e compreensivo da decisão, iluminado pela jurisprudência anterior do TC e articulando-a com a jurisprudência do Tribunal de Justiça da União europeia.

[Received/Recebido: novembro 21, 2022; Accepted/Aceito: janeiro 25, 2023]

Resultados: A decisão do Tribunal Constitucional põe termo ao entendimento generalizado (mas não unânime) da jurisprudência portuguesa anterior, no sentido de a legislação portuguesa sobre retenção e utilização de metadados como instrumento de investigação criminal não ter sido afectada pela declaração de invalidade da directiva europeia que esteve na sua origem, reconhecendo que a retenção generalizada de metadados de comunicações electrónicas é, em si mesma, violadora de direitos fundamentais vários, independentemente das garantias legais que rodeiam a utilização desses metadados.

Contribuições: O presente trabalho destaca as dificuldades que a tecnologia coloca ao Direito e aos juristas, ao mesmo tempo que salienta a necessidade de ponderar adequadamente os riscos da sua utilização. A existência de benefícios evidentes não é suficiente para justificar essa utilização quando a mesma comporte riscos de ofensa grave a direitos fundamentais.

Palavras-Chave: Comunicações electrónicas; Metadados; Direitos Fundamentais; Respeito pela vida privada.

ABSTRACT

***Objectives**: The present work aims to analyze the difficulties raised by electronic communications metadata as a criminal investigation tool, based on the recent Judgment of the Portuguese Constitutional Court No. 268/2022, of June 3rd.*

***Methodology**: an analytical and comprehensive study of the decision is carried out, illuminated by the previous case law of the Portuguese Constitutional Court in articulation with the case law of the Court of Justice of the European Union.*

***Results**: The Constitutional Court decision puts an end to the widespread (but not unanimous) understanding of the previous Portuguese jurisprudence according to which Portuguese legislation on retention and use of metadata as a tool for criminal investigation was not affected by the declaration of invalidity of the European directive that was in its origin, recognizing that the widespread retention of electronic communications metadata is, in itself, a violation of several fundamental rights, regardless of the legal guarantees surrounding the use of such metadata.*

***Contributions**: the present paper highlights the difficulties that technology poses to Law and jurists, emphasizing, at the same time, the need to adequately reflect about the risks of its use. The existence of obvious benefits is not sufficient to justify such use when it involves risks of serious harm to fundamental rights.*

***Keywords**:* Electronic communications; Metadata; Fundamental rights; Respect for private life.

[Received/Recebido: novembro 21, 2022; Accepted/Aceito: janeiro 25, 2023]

"[an illusory conviction that] global surveillance is the deus ex machina capable of combating the scourge of global terrorism".[1]

1 INTRODUÇÃO

O Tribunal Constitucional português é o único órgão com competência para declarar, com força obrigatória geral (fiscalização abstracta), a inconstitucionalidade de normas jurídicas, ainda que todos os tribunais possam (e devam) proceder à fiscalização da constitucionalidade das normas que violem disposições da lei fundamental (fiscalização concreta), embora a decisão apenas valha no próprio caso.

No caso de declarar a inconstitucionalidade com força obrigatória geral, o Tribunal Constitucional pode limitar os efeitos da declaração de inconstitucionalidade, designadamente prevendo a eficácia *ex nunc* da decisão (282.º, n.º 4 da CRP). A regra, porém, é a da eficácia *ex tunc*, isto é, a decisão retroage os seus efeitos à data de início de vigência da norma inconstitucional (ou ao momento em que esta se tornou inconstitucional, tratando-se de inconstitucionalidade superveniente), de acordo com o artigo 282.º, n.ºs 1 e 2 da Constituição da República Portuguesa.

Em 2008, através da Lei n.º 32/2008, de 17 de Julho, Portugal procedeu à transposição da Directiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de Março, lei que ficou conhecida como Lei dos Metadados.

A referida Lei impõe aos fornecedores de serviços de comunicações electrónicas publicamente disponíveis ou de uma rede pública de comunicações a conservação de uma série de dados relativos a comunicações electrónicas (metadados), pelo período de um ano e, bem assim, a transmissão desses dados às autoridades, mediante despacho de juiz de instrução criminal, a requerimento do

[1] PAULO PINTO DE ALBUQUERQUE, voto de vencido no Acórdão do TEDH, proferido no caso *Szabó e Vissy contra Hungria*, de 12 de Janeiro de 2016, proc. 37138/14. O caso de que se retirou a citação diz respeito à utilização de metadados por serviços de informação e segurança ("serviços secretos"). Em Portugal várias iniciativas legislativas para permitir esse tipo de acesso foram bloqueadas pelo Tribunal Constitucional. Para mais desenvolvimentos sobre o tema – que não será abordado neste artigo, vide (MACHADO, M. Gomes, 2019).

[Received/Recebido: novembro 21, 2022; Accepted/Aceito: janeiro 25, 2023]

Ministério Público e/ou da polícia criminal competente, no âmbito da investigação de criminalidade grave.

Entre os dados a conservar e transmitir encontram-se dados de tráfego e de localização relativos a todas as comunicações electrónicas (ou sua tentativa), designadamente os necessários para encontrar e identificar a fonte e o destino de uma comunicação, a data, a hora e a duração, o tipo de comunicação, o equipamento de telecomunicações dos utilizadores e a localização do equipamento de comunicação móvel (mas não o conteúdo das comunicações). O tipo de dados concretos a reter e a transmitir depende do tipo de comunicação (telefónica, por correio electrónico ou outra forma de comunicação através da internet), mas são sempre dados bastante detalhados. Além dos dados de tráfego e de localização, são igualmente conservados (e transmitidos) os chamados dados de base (dados relativos à conexão à rede).

No que toca à afectação de direitos fundamentais, como consequência do regime previsto naquela lei, é possível identificar dois momentos de possível lesão de direitos: i) o primeiro é o da *recolha e conservação* dos referidos dados, potencialmente lesivos de direitos como a reserva da intimidade da vida privada ou da inviolabilidade das comunicações e, ii) o segundo é o momento da *transmissão* dos referidos dados às autoridades judiciárias, sem necessidade de comunicação ao visado, potencialmente violadora ainda do direito à tutela jurisdicional efectiva (direito de defesa), por impossibilidade de controlo do modo como os dados foram recolhidos, tratados e transmitidos.

A Provedora de Justiça requereu ao Tribunal Constitucional a fiscalização abstracta da constitucionalidade das três disposições mais relevantes da referida lei em 2019 (artigo 4.º, relativo aos dados a conservar, art.º 6.º, relativo ao período de conservação e art.º 9.º, relativo à transmissão de dados).

O Tribunal Constitucional viria a declarar inconstitucionais as referidas normas, através do Acórdão n.º 268/2022, de 3 de Junho[2], sem limitar os efeitos da

[2] O Acórdão é de 19 de Abril. A data oficial é a da publicação em Diário da República.

[Received/Recebido: novembro 21, 2022; Accepted/Aceito: janeiro 25, 2023]

declaração (isto é, com eficácia *ex tunc*), tornando não só mais difícil (ou impossível) a utilização deste tipo de dados para o futuro, mas com consequências não totalmente previsíveis para os casos já julgados, em que os referidos dados tenham sido utilizados e tenham sido determinantes para a condenação.[3]

Na verdade, o acesso aos dados de tráfego é habitualmente requerido em momento posterior à tomada de conhecimento dos factos criminosos, com a notícia do crime, no início da investigação criminal, pelo sempre será em momento posterior à sua prática. Pelo que, se não forem conservados pelas operadoras não são acedíveis *a posteriori*.[4]

2 ANTECEDENTES

Como se referiu já, a Lei 32/2008 procedeu à transposição da Directiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de Março, ainda que, de acordo com a jurisprudência maioritária em Portugal, as limitações à utilização dos metadados recolhidos na investigação criminal acrescentadas pelo legislador português tornassem a lei portuguesa mais conforme às normas e princípios

[3] Nos termos do art.º 449.º do Código de Processo Penal (CPP), que permite a reabertura do processo se for "declarada, pelo Tribunal Constitucional, a inconstitucionalidade com força obrigatória geral de norma de conteúdo menos favorável ao arguido que tenha servido de fundamento à condenação". Tem legitimidade para requerer a revisão, além do condenado, o Ministério Público (artigo 450º, nº 1, al a) e c) do CPP.

[4] PEDRO VERDELHO (2010, p. 410) admite: "O pano de fundo do crime do artigo 13.º da Lei 32/2008 é a detalhada regulamentação, constante deste diploma legal, dos procedimentos de conservação dos chamados dados de tráfego. Como já se disse, a obrigação de conservação de certos dados referentes a comunicações, por parte dos fornecedores de serviços de comunicações electrónicas é o principal objectivo da Lei nº 32/2008. Porém, este objectivo não vale em si mesmo. Na verdade, como claramente resulta do n.º 1 do artigo 3.º da lei, a conservação de dados "tem por finalidade exclusiva a investigação, detecção e repressão de crimes graves por parte das autoridades competentes". Essa transmissão de dados, nos termos do n.º 2 do mesmo artigo 3.º, "só pode ser ordenada ou autorizada por despacho fundamentado do juiz", sendo certo que apenas assim poderá acontecer "se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter no âmbito da investigação, detecção e repressão de crimes graves" (artigo 9º, nº 1 da Lei nº 32/2008)". Sobre este tem, veja veja-se ainda ALEXANDRE DIAS PEREIRA (2019).

[Received/Recebido: novembro 21, 2022; Accepted/Aceito: janeiro 25, 2023]

fundamentais que consagram direitos humanos (quer de direito interno, quer de direito da União ou de direito internacional) do que a directiva que lhe deu origem.

A Directiva 2006/24/CE foi considerada inválida pelo Tribunal de Justiça da União Europeia (TJUE) no famoso caso *Digital Rights Ireland* (de 8 de Abril de 2014, processos apensos C-293/12 e C-594/12)[5].

A directiva abrangia todos aqueles que utilizassem serviços de comunicações electrónicas no espaço da União Europeia, independentemente de as pessoas cujos dados eram conservados se encontrarem numa situação susceptível de dar lugar a procedimentos penais. A directiva não previa também qualquer diferenciação, limitação ou excepções em função do objectivo de luta contra as infracções graves, pelo que era aplicável mesmo a pessoas cujas comunicações estivessem sujeitas ao segredo profissional.

A directiva, à semelhança (pelo menos, aparentemente[6]) da lei portuguesa, não impunha que os dados em causa fossem conservados no território da União, pelo que não se podia considerar que estivesse plenamente garantida a fiscalização da sua conservação por uma entidade independente.

Na referida decisão, o TJUE entendeu, assim, que a obrigação imposta pela Directiva 2006/24/CE aos fornecedores de serviços de comunicações electrónicas constituía uma violação dos artigos 7**.°** (protecção da vida privada) e 8.° (protecção de dados pessoais) da Carta dos Direitos Fundamentais da União Europeia (CDFUE).

Nesta medida, o TJUE concluiu que a Directiva 2006/24/CE não previa garantias suficientes, como exige o artigo 8.° da CDFUE, que permitissem assegurar uma protecção eficaz dos dados conservados contra os riscos de abuso e contra qualquer acesso e utilização ilícita dos mesmos. Ao adoptar a Directiva 2006/24/CE, o legislador da União teria excedido os limites impostos pelo princípio da proporcionalidade à luz dos artigos 7.°, 8.° e 52.°, n.° 1, da CDFUE, razão pela qual o

[5]Disponível em em https://eur-lex.europa.eu/legalcontent/PT/TXT/HTML/?uri=CELEX:62012CJ0293&from=EN

[6] Na declaração de voto, o Conselheiro LINO RIBEIRO considera que a remissão operada pelo artigo 7.º, n.º 4, da Lei 32/2008 para a lei de protecção de dados implica que os dados tenham de estar conservados em território da União e, no caso dos operadores nacionais, em território português.

[Received/Recebido: novembro 21, 2022; Accepted/Aceito: janeiro 25, 2023]

TJUE declarou a invalidade da directiva na sua totalidade, sem reservas quanto aos efeitos temporais da sua decisão (eficácia *ex tunc*).

A decisão do TJUE colocou de imediato o problema dos efeitos da invalidade da directiva nos diplomas nacionais que procederam à sua transposição para os direitos internos dos Estados-Membros (no caso português, a referida Lei n.º 32/2008).

Ora, resulta da jurisprudência assente do TJUE que as autoridades nacionais: i) não devem aplicar, sob pena de incumprimento do direito da União, uma disposição normativa europeia considerada inválida pelo TJUE; e ii) devem deduzir no seu ordenamento interno as consequências de uma declaração de invalidade de uma disposição europeia pelo TJUE (SILVEIRA & FREITAS, 2017, p. 52).

Todavia, na sequência do acórdão *Digital Rights Ireland*, o Ministério Público português emitiu uma nota prática, na qual se afirma:

> É importante sublinhar que a Lei 32/2008, além da transposição da Diretiva 2006/24/CE, introduziu um mais alargado quadro, muito complexo, de regulamentação do processo de retenção de dados […]. Neste exercício, a lei nacional foi muito para lá das exigências da Directiva. Desta forma, a maior parte das exigências que vieram a ser feitas pelo acórdão do TJUE estariam já anteriormente consideradas no direito interno. Por essa razão, tem sido entendido que a decisão do tribunal do Luxemburgo não afeta a validade da lei nacional. (GABINETE CIBERCRIME, 2015)[7]

Este entendimento foi seguido pela maioria dos Tribunais portugueses até ao momento, com algum apoio da doutrina (RAMALHO & COIMBRA, 2015, pp. 1037 e ss.).

Porém, em Outubro de 2016, o Tribunal de Instrução Criminal de Lisboa recusou um pedido de acesso a metadados de comunicações (“autorização de transmissão dos dados de identificação de um utilizador a quem estava atribuído um determinado endereço de protocolo IP”) efectuado pelo Ministério Público, com

[7]Disponível em: https://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/nota_pratica_7_retencao_de_dados.pdf (consultado a 24/07/2022).

[Received/Recebido: novembro 21, 2022; Accepted/Aceito: janeiro 25, 2023]

fundamento na inconstitucionalidade do artigo 6.º (por referência ao artigo 4.º) da Lei 32/2008, por violação dos art.ºs 18.º e 34.º, n.º 4, da Constituição.

O Ministério Público recorreu para o Tribunal Constitucional, que viria a considerar, em processo de fiscalização concreta da constitucionalidade, no Acórdão 420/2017, de 29 de Setembro[8], que a referida norma *não era inconstitucional*[9].

Em 2017, a Comissão Nacional de Protecção de Dados (CNPD), entidade competente para instruir os processos de contraordenação por violação da Lei 32/2008, adoptou uma deliberação (Deliberação 1008/2017, de 18 de Julho[10]), pela qual decidiu não aplicar a referida Lei aos processos que lhe fossem submetidos (nomeadamente as queixas do Ministério Público por recusa de colaboração na transmissão de metadados pelos operadores de telecomunicações, nos termos definidos na Portaria n.º 469/2009, de 6 de Maio), por entender que a lei portuguesa violava a Carta dos Direitos Fundamentais da União Europeia.

Um pouco antes, a 21 Dezembro de 2016, no caso *Tele2*[11], o TJUE considerou incompatível com o direito da União a existência de:

> regulamentação nacional que prevê, para efeitos de luta contra a criminalidade, uma conservação generalizada e indiferenciada de todos os dados de tráfego e dados de localização de todos os assinantes e utilizadores registados em relação a todos os meios de comunicação electrónica.

[8] Texto integral disponível em http://www.tribunalconstitucional.pt/tc/acordaos/20170420.html?impressao=1

[9] No caso, estava (no entendimento do Tribunal), apenas em causa a utilização dos chamados dados de base, isto é, dos dados que constituem "elementos necessários ao estabelecimento de uma base para comunicação, que estão aquém, antes, são prévios e instrumentos de qualquer comunicação", relativamente aos quais não são se aplicam as mesmas exigências relativas aos dados de tráfego e de localização. O Tribunal acompanhou, nesta parte, a posição de COSTA ANDRADE (2008, p. 341), segundo o qual "a pertinência dos dados à categoria e ao regime das telecomunicações pressupõe, em qualquer caso, a sua vinculação a uma concreta e efetiva comunicação ao menos tentada/falhada entre pessoas", o que não sucede com os dados de base considerados em si mesmos. Assim, o juízo de inconstitucionalidade ali formulado não é necessariamente contraditório com o juízo de inconstitucionalidade proferido no acórdão 268/2022.

[10] Disponível em file:///C:/Users/4701/Downloads/20_1008_2017%20(1).pdf (consultado a 24/07/2022).

[11] Processos apensos C-203/15 e C-698/15.

[Received/Recebido: novembro 21, 2022; Accepted/Aceito: janeiro 25, 2023]

Com efeito, o n.º 1 do art.º 15.º da Directiva **2002/58/CE**, do Parlamento e do Conselho, de 12 de Julho de 2002, previa:

> Os Estados-Membros podem adotar medidas legislativas para restringir o âmbito dos direitos e obrigações previstos nos artigos 5.° e 6.°, nos n.os 1 a 4 do artigo 8.º e no artigo 9.º da presente diretiva sempre que essas restrições constituam uma medida necessária, adequada e proporcionada numa sociedade democrática para salvaguardar a segurança nacional (ou seja, a segurança do Estado), a defesa, a segurança pública, e a prevenção, a investigação, a deteção e a repressão de infrações penais ou a utilização não autorizada do sistema de comunicações eletrónicas […]. Para o efeito, os Estados-Membros podem designadamente adotar medidas legislativas prevendo que os dados sejam conservados durante um período limitado, pelas razões enunciadas no presente número. Todas as medidas referidas no presente número deverão ser conformes com os princípios gerais do direito comunitário, incluindo os mencionados nos n.os 1 e 2 do artigo 6.º do Tratado da União Europeia.

De acordo com o TJUE, porém, o "artigo 15.º, n.º 1, da Directiva 2002/58 […] lido à luz dos artigos 7.°, 8.° e 11.° bem como do artigo 52.º, n.º 1, da Carta dos Direitos Fundamentais, deve ser interpretado no sentido de que se opõe a uma regulamentação nacional que":

> [...] prevê, para efeitos de luta contra a criminalidade, uma conservação generalizada e indiferenciada de todos os dados de tráfego e dados de localização de todos os assinantes e utilizadores registados em relação a todos os meios de comunicação eletrónica" "[...] regula a proteção e a segurança dos dados de tráfego e dos dados de localização, em especial, o acesso das autoridades nacionais competentes aos dados conservados, sem limitar, no âmbito da luta contra a criminalidade, esse acesso apenas para efeitos de luta contra a criminalidade grave, sem submeter o referido acesso a um controlo prévio por parte de um órgão jurisdicional ou de uma autoridade administrativa independente, e sem exigir que os dados em causa sejam conservados em território da União.

Entende assim o TJUE ser possível a recolha e utilização de metadados, mas apenas num quadro legal que limite selectivamente a *recolha* (isto é, a uma recolha não indiscriminada de todos os dados de todos os utilizadores), à conservação dos dados no território da união e sujeitando a transmissão desses dados a situações de

[Received/Recebido: novembro 21, 2022; Accepted/Aceito: janeiro 25, 2023]

combate à criminalidade grave e ao controlo prévio de uma autoridade jurisdicional ou administrativa independente.

3 CONTEÚDO DECISÓRIO DO ACÓRDÃO DO TC

O TC considerou inconstitucionais as normas da Lei n.º 32/2008 relativas às categorias de dados a conservar conjugadas com o período de conservação de um ano (artigos 4.º e 6.º), salientando que a lei não prevê o armazenamento desses dados em Portugal ou noutro Estado-Membro da União Europeia, pelo que põe em causa o direito de o visado controlar o tratamento dos dados a seu respeito, bem como a efectividade da garantia constitucional de fiscalização por uma autoridade administrativa independente.

Além disso, o TC considerou que uma obrigação indiferenciada e generalizada de armazenamento de todos os dados de tráfego e localização (metadados) relativos a todas as pessoas - que revelam a todo o momento aspectos da vida privada e familiar dos cidadãos, permitindo rastrear a localização do indivíduo todos os dias e ao longo do dia e identificar com quem contacta, a duração e a regularidade dessas comunicações -, restringe de modo desproporcionado os direitos à reserva da intimidade da vida privada e à autodeterminação informativa. Com efeito, a lei atinge sujeitos relativamente aos quais não existe qualquer suspeita de actividade criminosa, já que se recolhem e conservam dados relativos a comunicações electrónicas da totalidade da população, sem qualquer diferenciação, excepção ou ponderação face ao objectivo perseguido.

Por outro lado, a norma relativa à transmissão de dados armazenados às autoridades competentes para investigação (artigo 9.º) foi igualmente considerada inconstitucional, 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 susceptível de comprometer as investigações nem a vida ou integridade física de terceiros. Em consequência, ao não

[Received/Recebido: novembro 21, 2022; Accepted/Aceito: janeiro 25, 2023]

se prever essa informação às pessoas atingidas, os visados ficam privados de exercer controlo efectivo sobre a licitude e regularidade daquele acesso, em violação dos direitos à autodeterminação informativa (na dimensão de controlo do acesso de terceiros a dados pessoais) e do direito (fundamental) a uma tutela jurisdicional efectiva.

Já depois de conhecida a decisão, a Procuradoria-Geral da República veio "arguir a nulidade do Acórdão", pretendendo que o TC fixasse a sua eficácia *ex nunc*, de modo a salvaguardar a manutenção das decisões judiciais já proferidas em que aqueles dados tivessem sido utilizados.

O TC rejeitou aquela pretensão, através do Acórdão n.º 382/2022[12], de 13 de Maio, por razões formais (ilegitimidade da PGR para suscitar incidentes pós-decisórios), acrescentando, porém, que:

> [...]as normas que determinam uma obrigação indiferenciada de conservação de metadados *não podiam já ser aplicadas por qualquer autoridade nacional desde 2014*, momento em que se concluiu pela sua incompatibilidade com a Carta dos Direitos Fundamentais da União Europeia (Acórdãos do Tribunal de Justiça da União Europeia de 8 de abril de 2014, *Digital Rights Ireland*, proc. C-293/12 e C-594/12; e de 21 de dezembro de 2016, *Tele2 Sverige e Watson*, proc. C-203/15 e C-698/15) e surgiu a obrigação, para *todas as autoridades nacionais* (incluindo judiciárias) de recusar a sua aplicação, nos termos do disposto no n.º 4 do artigo 8.º da Constituição". [o destaque em itálico consta do original].

4 CONSIDERAÇÕES FINAIS

A conservação em massa de metadados de comunicações electrónicas pelos operadores e o seu (relativamente) fácil acesso pelos operadores judiciários tornaram aqueles dados uma importante ferramenta de combate à criminalidade.

Os tribunais portugueses continuaram a aplicar, perante a passividade do legislador, disposições legais contrárias ao Direito da União Europeia, pelo menos

[12] Disponível em: https://www.tribunalconstitucional.pt/tc/acordaos/20220382.html (consultado a 24/07/2022).

[Received/Recebido: novembro 21, 2022; Accepted/Aceito: janeiro 25, 2023]

desde 2014, sendo certo que a decisão do TJUE no caso *Digital Rights Ireland* não limitou temporalmente os seus efeitos, pelo que estes retroagem à data de início da vigência da Directiva transposta pela Lei n.º 32/2008.

A lei portuguesa foi mais exigente do que a Directiva que lhe deu origem no que respeita à *transmissão* dos metadados, designadamente sujeitando-a a autorização judicial. No entanto, a lei portuguesa, à semelhança da Directiva, não só permitia como prescrevia a *recolha* indiscriminada de metadados de localização e de tráfego, algo que os juízes do TJUE consideraram incompatível com a Carta dos Direitos Fundamentais.

A declaração de inconstitucionalidade com força obrigatória geral levará à reabertura de processos judiciais em que tenham sido utilizados metadados (que agora se consideram conservados e acedidos de forma ilegítima em virtude da declaração de inconstitucionalidade), bem como à nulidade de provas obtidas pelos mesmos meios em processos em curso, o que representa um custo para o sistema judicial e, potencialmente, para a segurança interna.

No entanto, além de constituir uma violação de *direitos individuais* – violação que serviu de fundamento à decisão do Tribunal Constitucional e, em larga medida, também às decisões do TJUE –, a recolha e conservação indiscriminada de metadados coloca problemas de outra ordem, de idêntica ou até de superior gravidade.

Imagine-se uma pessoa com acesso (legítimo ou ilegítimo) aos dados que pretende identificar os indivíduos que se opõem à política do governo em funções. A exploração dos metadados de comunicações permitiria identificar, quase instantaneamente, todos os indivíduos inscritos em listas de distribuição de mensagens de correio electrónico que criticam a política do governo, ou todos os indivíduos que participam em manifestações públicas de oposição ao governo[13] ou

[13] Exemplos retirados das conclusões do Advogado-Geral HENRIK SAUGMANDSGAARD ØE no Caso *Tele2*, disponíveis em: https://curia.europa.eu/juris/document/document.jsf;jsessionid=26A57FD2876E7537DD6A04193277B8D1?text=&docid=181841&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=1550113 .

[Received/Recebido: novembro 21, 2022; Accepted/Aceito: janeiro 25, 2023]

que participaram em reuniões de partidos de oposição, o que constitui um risco inaceitável numa sociedade democrática, risco porventura superior ao do acesso ao conteúdo das comunicações, pela sua natureza mais difíceis de analisar de forma rápida e sistemática.

O contributo da tecnologia e, em particular dos metadados, para a segurança pública e para o combate à criminalidade é inegável. No entanto, o respeito pelos direitos humanos obriga os legisladores a rodearem de cautelas a sua utilização, devendo prever (e acautelar, até ao limite do possível), que esses dados não possam ser utilizados indevidamente.

Numa conferência recente organizada pelo *Swiss Federal Institute for NBC (nuclear, biological and chemical) Protection – Spiez Laboratory,* os investigadores ali reunidos discutiram as possibilidades do mau uso de tecnologias de ponta na área da biotecnologia e da química, pegando no exemplo da utilização de inteligência artificial para a simulação de novos compostos químicos, usada, designadamente, pela indústria farmacêutica para o desenvolvimento de novos medicamentos. Um algoritmo utilizado por uma das empresas participantes gerou, em menos de 6 horas, mais de 40.000 moléculas potencialmente perigosas, incluindo algumas já existentes que correspondem a algumas das armas químicas mais poderosas que se conhecem, como o Agente nervoso VX (URBINA *et al*., 2022, p.189).

Paralelamente, a existência de bases de dados maciças e indiscriminadas de metadados de comunicações representa, por isso e por si só, um risco significativo para os direitos humanos, devendo, consequentemente, a sua própria existência ser objecto de reflexão. Em todo o caso, a jurisprudência quer do TJUE quer do TC português parece impedir o próprio legislador de prever a existência de tais bases de dados.

[Received/Recebido: novembro 21, 2022; Accepted/Aceito: janeiro 25, 2023]

REFERÊNCIAS

COSTA ANDRADE, Manuel da. Bruscamente no Verão Passado: a Reforma do Código de Processo Penal. **Revista de Legislação e Jurisprudência**, Ano 137.º, n.º 3951, pp. 318-355, 2008.
MACHADO, M. Gomes. **O acesso aos metadados pelos Serviços de Informações da República Portuguesa**, Coimbra: Almedina, 2019.

PEREIRA, Alexandre Dias. Direito ao respeito pela vida privada digital, in **Comentário à Convenção Europeia dos Direitos Humanos e dos Protocolos Adicionais**, coord. Paulo Pinto de Albuquerque, pp. 1449-1470, Lisboa: Universidade Católica Editora, 2019.

RAMALHO, D. S., COIMBRA, J. D. 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. **O Direito**, n.º 147.º, IV, pp. 997-1045, (2015).

SILVEIRA, A; FREITAS, P. M. Implicações da declaração de invalidade da Diretiva 2006/24 na conservação de dados ("metadados") nos Estados-Membros da UE: uma leitura jusfundamental. **Revista de Direito, Estado e Telecomunicações**, Brasília, v. 9, n.º 1, p. 47-68, 2017. DOI: https://doi.org/10.26512/lstr.v9i1.21513

VERDELHO, Pedro, Anotação ao artigo 13º da Lei 32/2008 de 17-7, em **Comentário das Leis Penais Extravagantes, vol.** 1, Paulo Pinto Albuquerque, José Branco (org.), Lisboa: Universidade Católica Editora, 2010.

URBINA, F., LENTZOS, F., INVERNIZZI, C., & Ekins, S. Dual use of artificial-intelligence-powered drug discovery. **Nature Machine Intelligence**, *4*(3), pp. 189–191, 2022. https://doi.org/10.1038/s42256-022-00465-9

[Received/Recebido: novembro 21, 2022; Accepted/Aceito: janeiro 25, 2023]