

Universidade Católica Portuguesa

Faculdade de Direito | Escola de Lisboa



CATOLICA
FACULDADE DE DIREITO

ESCOLA DE LISBOA

**A CONSERVAÇÃO E O ACESSO A METADADOS PARA FINS
DE INVESTIGAÇÃO CRIMINAL**

Flávia Fidalgo Torres da Costa

Dissertação elaborada no âmbito do Mestrado em Direito Forense

Sob orientação do Professor Doutor Henrique Salinas

Oslo, 28 de março de 2024

*Stol på livets prosess,
du er akkurat der du skal være.
(Confia no processo da vida,
Tu estás exatamente onde deverias estar.)*

Agradecimentos

Aos meus pais, sem os quais nada disto seria possível.

À minha mãe, que está *sempre* comigo, pela especial maturidade que me fez adquirir desde pequena e por celebrar as minhas conquistas como se dela fossem (e que, na verdade, *são*). Por toda a força, ajuda e apoio incondicional, obrigada.

Ao meu pai, pelo rigor e exigência e por nunca me deixar desistir.

Aos restantes familiares, por sempre me acompanharem. Um agradecimento especial ao meu irmão Filipe, a quem estou grata não só pela ajuda que me proporcionou, como também por toda a calma e paz que transmite. Agradeço, também, à D.^a Laura, por me encorajar a seguir os meus sonhos e a ser feliz.

A todos os meus amigos, por me terem acompanhado neste percurso e por me mostrarem o lado leve da vida. Em especial, à Mariana, à Jéssica e à Bárbara, por todos os momentos partilhados e pela amizade única que construímos.

À minha professora primária, Aurora Dias, de quem ainda hoje me lembro, por ter sido fundamental no desenvolvimento da minha autoconfiança.

Ao Dr. Marco Rosa e ao Sr. Embaixador Pedro Pessoa e Costa, pela compreensão e atenção.

Ao Professor Henrique Salinas, pela sua orientação.

Por último, mas não menos importante,

Til Roman, som fulgte og støttet meg gjennom hele prosessen. Tusen takk for all din kjærlighet og hengivenhet. Jeg er veldig glad for å ha deg i livet mitt.

Resumo

No atual contexto digital, onde a fronteira entre o mundo físico e o mundo digital se mostra cada vez mais ténue, os instrumentos tradicionais processuais não se revelam aptos a dar resposta ao combate à criminalidade grave.

O acesso a metadados, possibilitado pela sua conservação, surge, assim, como um meio de aquisição probatória adaptado à realidade atual e indispensável para a investigação de certos crimes. Contudo, restringindo este meio de obtenção de prova importantes direitos fundamentais, a busca pela concordância prática entre o dever do Estado em garantir a segurança e a necessária tutela dos direitos restringidos revela-se crucial.

A questão é perceber até que ponto é tolerável a restrição de direitos, liberdades e garantias de certo grupo de cidadãos em nome de um valor constitucionalmente protegido, como a segurança, que afeta toda a comunidade.

Palavras-Chave: metadados; conservação e acesso; direitos fundamentais; princípio da proporcionalidade; investigação criminal.

Abstract

In today's digital context, where the line between the physical and digital world is becoming increasingly blurred, traditional procedural tools are not adequate to fight serious crime.

Access to metadata, provided by its retention, has therefore emerged as a means of acquiring evidence adapted to the current reality and essential for investigating certain crimes. However, since this means of obtaining proof restricts important fundamental rights, the search for a balance between the State's duty to guarantee security and the necessary protection of the rights being restricted is crucial.

The question is to understand to what extent the restriction of rights, freedoms and guarantees of a certain group of citizens is tolerable in the name of a constitutionally protected value, such as security, which affects the entire community.

Keywords: metadata; retention and access; fundamental rights; principle of proportionality; criminal investigation.

Siglas e Abreviaturas

abr. – abril

Ac./ Acs. – Acórdão/Acórdãos

al. – alínea

AR – Assembleia da República

art./arts. – artigo/artigos

BE – Bloco de Esquerda

CDFUE – Carta dos Direitos Fundamentais da União Europeia

cfr. – confira

cit. – citada

CNPD – Comissão Nacional de Proteção de Dados

CPP – Código de Processo Penal

CRP – Constituição da República Portuguesa

dez. – dezembro

DUE – Direito da União Europeia

ed. – edição

EM – Estado-Membro

et al. – *et alia* (e outros)

ex. – exemplo

FDUL – Faculdade de Direito da Universidade de Lisboa

IL – Iniciativa Liberal

IMEI - *International Mobile Equipment Identity* (Identidade Internacional do Equipamento Móvel)

IMSI - *International Mobile Subscriber Identity* (Identidade Internacional de Assinante Móvel)

IP – *Internet Protocol* (Protocolo de Internet)

jan. – janeiro

JIC – Juiz de Instrução Criminal

jul. – julho

jun. – junho

LC – Lei do Cibercrime

LOSJ – Lei de Organização do Sistema Judiciário

mar. – março

MP – Ministério Público

n.º/n.ºs – número/números
out. – outubro
p./pp. – página/páginas
PCP – Partido Comunista Português
PGR – Procuradoria Geral da República
PR – Presidente da República
Proc./Procs. – Processo/Processos
PS – Partido Socialista
PSD – Partido Social Democrata
RGPD – Regime Geral de Proteção de Dados
set. – setembro
ss. – seguintes
STJ – Supremo Tribunal de Justiça
TC – Tribunal Constitucional
TJUE – Tribunal de Justiça da União Europeia
TRC – Tribunal da Relação de Coimbra
TRE – Tribunal da Relação de Évora
TRG – Tribunal da Relação de Guimarães
TRL – Tribunal da Relação de Lisboa
TRP – Tribunal da Relação do Porto
TUE – Tratado da União Europeia
UCP – Universidade Católica Portuguesa
vol. – volume

Índice

Introdução.....	8
Capítulo I – Considerações Preliminares.....	10
1. O que são metadados?	10
2. Evolução legislativa até à Lei do Cibercrime.....	13
Capítulo II – Da jurisprudência do TJUE.....	18
1. O Acórdão <i>Digital Rights Ireland</i>	18
2. A posterior <i>reorientação</i> da posição do TJUE.....	21
Capítulo III – Do impacto do DUE na ordem jurídica interna	24
1. O Acórdão do TC n.º 268/2022	24
2. Após a declaração de inconstitucionalidade do cerne da Lei n.º 32/2008.....	27
Capítulo IV – Análise Crítica	29
1. Os direitos fundamentais em discussão	29
2. A conservação dos dados de tráfego e de localização	31
3. A adoção da Lei n.º 18/2024.....	42
Conclusões.....	44
Referências	47

Introdução

Num contexto de crescente evolução tecnológica e digitalização da sociedade, o crime tem vindo a adotar práticas mais sofisticadas e complexas, colocando novos desafios à investigação criminal, sobretudo no que diz respeito ao combate à criminalidade grave.

Para fazer face a esta nova natureza de crimes, os meios tradicionais de aquisição probatória, revelam-se, hoje, insuficientes, exigindo-se o recurso a novos métodos de investigação, como a conservação e acesso a metadados, possibilitados, igualmente, pelo avanço da tecnologia.

Neste quadro, importa partir de duas premissas, imprescindíveis para a análise desta dissertação.

Em primeiro lugar, não existe Estado de Direito Democrático sem autoridades de investigação criminal dotadas de meios capazes para prevenir e sancionar eficazmente o cometimento de crimes, sob pena de se criarem insuportáveis vazios de punição. Esta é a prioridade de um Estado de Direito, não havendo liberdade sem segurança.

Contudo, e em segundo lugar, isto não significa que as autoridades de investigação criminal possam fazer tudo em nome do fim que prosseguem. O Direito Processual Penal, enquanto “direito constitucional aplicado”¹, não procura a verdade a todo o preço, tendo de respeitar os princípios e direitos fundamentais da Constituição.

Desempenhando a conservação e acesso a metadados um papel central na investigação de certos crimes, o objeto desta dissertação não diz respeito à discussão da sua existência, mas das condições em que os mesmos se devem processar. Isto porque, este meio de obtenção de prova implica a restrição de importantes direitos fundamentais.

Tendo presente que vivemos, hoje, numa sociedade de risco, onde existe uma maior predisposição para os direitos serem violados, apresentamos como objetivo alcançar a concordância prática entre o interesse do Estado na prossecução penal dos agentes do crime e a tutela adequada dos direitos, liberdades e garantias do cidadão.

Numa altura em que o TJUE atribui um alcance inédito aos direitos à privacidade e à proteção de dados, revela-se absolutamente necessário perceber de que forma a sua posição influencia a ordem interna e se se apresenta como a mais adequada.

¹ FIGUEIREDO DIAS, *Direito Processual Penal*, vol. I, Coimbra, Coimbra Editora, 1974, p. 74.

Por razões de economia, centraremos a nossa análise crítica na questão mais controversa dentro desta temática: o regime de conservação de dados de tráfego e de localização.

Capítulo I – Considerações preliminares

1. O que são metadados?

Os metadados são tidos como “dados sobre os dados comunicados”, gerados “antes e durante o processo de comunicação” e que estão na posse dos fornecedores de serviços de telecomunicações². São, por isso, “tratados (...) para efeitos de transmissão, distribuição ou intercâmbio de conteúdo de comunicações eletrónicas”³, contendo informação sobre localização, data, duração, tipo de comunicação, fonte e destino dos atos efetuados através de telecomunicações ou outros meios de comunicação⁴⁻⁵.

No que toca aos dados respeitantes às telecomunicações, em Portugal, é tradicionalmente utilizada uma classificação tripartida, que consta na lei, distinguindo três categorias de dados: dados de base, dados de tráfego e dados de conteúdo⁶.

Os metadados não são o conteúdo comunicado⁷, pelo que apenas as duas primeiras categorias de dados serão objeto da nossa análise.

Começando pelos dados de base, estes dizem respeito aos “elementos necessários ao acesso à rede, designadamente através da ligação individual e para utilização do próprio serviço”⁸, ou seja, independentemente de qualquer comunicação. Referimo-nos, aqui, à identificação do utilizador, morada, número de acesso e outros dados através dos quais o utilizador tem acesso ao serviço⁹. Estamos perante “dados fornecidos no âmbito de uma relação contratual e que se reportam a uma fase anterior a qualquer comunicação”, sendo obtidos para que a mesma se concretize¹⁰.

² RUI CARDOSO, “A conservação e a utilização probatória de metadados de comunicações eletrónicas após o Acórdão do Tribunal Constitucional n.º 268/20220 – o que nasce torto...”, in *Revista do Ministério Público*, n.º 172, out.-dez. 2022, p. 10.

³ Art. 4.º, n.º 3, al. c) da Proposta de Regulamento do Parlamento Europeu e do Conselho relativo ao respeito pela vida privada e à proteção de dados pessoais nas comunicações eletrónicas e que revoga a Diretiva 2002/58/CE, de 10/01/2017, disponível em: <https://eur-lex.europa.eu/homepage.html>.

⁴ Veja-se o Ac. TC n.º 403/2015, Proc. n.º 773/15, 9, disponível em: <http://www.tribunalconstitucional.pt>;

⁵ Destes dados não fazem parte os que estão na posse dos fornecedores de serviços *online*, como o *Facebook* (o que aí se publica ou comenta, por ex.). – cfr. RUI CARDOSO, “A conservação (...)”, cit., p. 11.

⁶ Veja-se o Parecer da PGR n.º 16/1994, disponível em: <https://www.ministeriopublico.pt/pareceres-pgr>. Esta classificação foi, desde logo, seguida pela jurisprudência – Acs. TC n.º 403/2015, Proc. n.º 773/15, n.º 420/2017, Proc. n.º 917/16, n.º 268/2022, Proc. n.º 828/2019, disponíveis em: <http://www.tribunalconstitucional.pt> e Ac. TRP de 22/02/2021, Proc. n.º 42003/20.8YIPRT-A.P1, Ac. TRG de 02/05/2023, Proc. n.º 12/23.6 PBGMR-A.G1, Ac. TRC de 12/10/2022, Proc. n.º 538/22.9JALRA.C1 e Ac. TRL de 11/10/2023, Proc. n.º 1232/19.3PBFUN.L1-3, disponíveis em: <http://www.dgsi.pt>.

⁷ Como o som, a imagem e o texto.

⁸ Ac. TC n.º 486/2009, Proc. n.º 4/09, 2.2, disponível em: <http://www.tribunalconstitucional.pt>.

⁹ Como o nome, data de nascimento, número de telefone, PIN e PUK.

¹⁰ TIAGO CAIADO MILHEIRO, “Artigo 189.º”, in *Comentário Judiciário do Código de Processo Penal*, Tomo II – Artigos 124.º a 190.º, Coimbra, Almedina, 2019, p. 826.

Os dados de tráfego, em contrapartida, são definidos como os “dados funcionais necessários ao estabelecimento de uma ligação ou comunicação e os dados gerados pela utilização da rede”¹¹. Reportam-se, assim, à direção, destino, trajeto, duração, data, hora e frequência de uma determinada comunicação, podendo, ainda, incluir a localização do interlocutor de origem e de destino¹².

Neste âmbito, é importante assinalar dois tópicos: um relativo à natureza dos dados de localização e outro referente ao endereço de protocolo IP (*Internet Protocol*).

Os dados de localização (art. 2.º, n.º 1, al. e) da Lei n.º 41/2004) podem enquadrar-se tanto nos dados de base, quando identificam a posição geográfica do aparelho, independentemente de qualquer comunicação, como nos dados de tráfego, quando esta identificação está associada a uma comunicação ou tentativa de comunicação, apresentando, assim, uma natureza híbrida¹³.

Não obstante, “nos dias de hoje ocorrem comunicações mesmo quando o utilizador do equipamento de comunicação não o aciona direta e intencionalmente”, nomeadamente quando atualiza o correio eletrónico ou recebe mensagens, pelo que as comunicações são “praticamente constantes”¹⁴.

A primeira espécie de dados de localização é, por isso, residual, tendo o TC defendido que a mesma se deve integrar no “conceito mais amplo de “dados de tráfego””¹⁵, posição com a qual concordamos.

Relativamente ao endereço de protocolo IP, a lei portuguesa não o classificou expressamente, dando origem a diferentes posições¹⁶.

DUARTE ALBERTO NUNES defende que se deve distinguir a situação em que está em causa um IP estático (que identifica permanentemente um ponto de acesso à rede) daquela em que se está perante um IP dinâmico (atribuído a um computador apenas quando se conexiona à rede e durante a sua ligação).

¹¹ Ac. TC n.º 403/2015, Proc. n.º 773/15, 9, disponível em: <http://www.tribunalconstitucional.pt>.

¹² Veja-se a definição presente no art. 2.º, al. c) da LC e no art. 2.º, n.º 1, al. d) da Lei n.º 41/2004. Estes dados podem ser subdivididos em duas categorias: i) dados de tráfego associados a atos de comunicação intersubjetiva e ii) dados de tráfego desligados de uma intercomunicação subjetiva, como a consulta de sítios na internet e os atos de comunicação entre uma pessoa e uma máquina. – cfr. Ac. TC n.º 464/2019, Proc. n.º 26/2018, 7, disponível em: <http://www.tribunalconstitucional.pt>.

¹³ Ac. TC n.º 268/2022, Proc. n.º 828/2019, 6.1, disponível em <http://www.tribunalconstitucional.pt>. Neste sentido, veja-se o Ac. TRC de 12/10/2022, Proc. n.º 538/22.9JALRA.C1, disponível em: <http://www.dgsi.pt>.

¹⁴ Parecer CNPD n.º 38/2017, disponível em: <https://www.cnpd.pt>.

¹⁵ Ac. TC n.º 268/2022, Proc. n.º 828/2019, 6.1, disponível em <http://www.tribunalconstitucional.pt>.

¹⁶ O mesmo acontece nos sistemas espanhol e alemão. – cfr. JOÃO CONDE CORREIA, “Prova Digital: as leis que temos e a lei que devíamos ter”, in *Revista do Ministério Público*, n.º 139, jul.-set. 2014, p. 48.

No primeiro caso, o Autor considera que estamos perante um dado de base, acessível pelo MP (art. 14.º da LC), enquanto, na segunda hipótese, já se estaria perante um dado de tráfego, já que o IP dinâmico está “associado a um concreto processo comunicacional”¹⁷⁻¹⁸.

O TC atende igualmente a esta distinção, tendo referido que “(...) a identificação do sujeito a que estava atribuído determinado *protocolo IP dinâmico* não permite, de forma tão clara, obedecer à divisão entre *dados de base* e *dados de tráfego*, pois certas circunstâncias da comunicação (a data e a hora) são inerentes à identificação do protocolo de IP dinâmico”¹⁹.

Neste contexto, alguma jurisprudência distingue, pelo contrário, as situações em que se pretende identificar o utilizador de um determinado endereço IP, num dado dia e hora, daquelas em que se pretende obter informação sobre um “alargado período de tempo” ou sobre “múltiplas comunicações”, entendendo que as primeiras se enquadram nos dados de base e as segundas nos dados de tráfego²⁰.

Finalmente, atendendo ao n.º 2 do art. 2.º da Lei n.º 32/2008²¹, tanto os dados de base, como os dados de tráfego e de localização são dados pessoais, nos termos do n.º 1 do art. 4.º do RGPD. Os dados de tráfego e de localização, ao permitirem “inferir, com precisão, informações detalhadas sobre padrões de vida individuais, círculos sociais de pertença, inclinações político-partidárias, bem como aspetos da vida pessoal, tais como rotinas, hobbies e vulnerabilidades (...)”²², são igualmente dados sensíveis (art. 9.º do RGPD)²³.

¹⁷ São salvaguardadas as situações em que, “conhecendo as autoridades qual o IP dinâmico utilizado, apenas esteja em causa saber quem utilizou aquele IP num dado momento”, tal constituindo a obtenção de um dado de base. – cfr. DUARTE RODRIGUES NUNES, *Os meios de obtenção de prova previstos na Lei do Cibercrime*, Coimbra, Gestlegal, 2018, pp. 62 e 63.

¹⁸ No sentido de que um protocolo de IP dinâmico é um dado de tráfego, veja-se o Ac. TRC de 13/10/2012, Proc. n.º 84/11.6JAGR-D.A.C1 e Ac. TRE de 27/01/2011, Proc. n.º 1276/09.3TAPTM-B.E1, disponíveis em: <http://www.dgsi.pt>.

¹⁹ Ac. TC n.º 268/2022, Proc. n.º 828/2019, 6.1, disponível em <http://www.tribunalconstitucional.pt>. Em sentido contrário, pronunciou-se o MP. – cfr. Nota Prática da PGR n.º 1/2012, disponível em: <https://cibercrime.ministeriopublico.pt/notas-praticas>.

²⁰ Nota Prática da PGR n.º 2/2013, disponível em: <https://cibercrime.ministeriopublico.pt/notas-praticas>. Veja-se o Ac. TRE de 13/11/2012, Proc. n.º 315/11.2PBPTG-A.E1 e Acs. TRL de 22/01/2013, Proc. n.º 581/12.6PLSNT-A.L1-5 e de 19/06/2014, Proc. n.º 1695/09.5PJLSB.L1-9, disponíveis em: <http://www.dgsi.pt>.

²¹ Alterado pela recente Lei n.º 18/2024.

²² Ponto 77.º do pedido de fiscalização abstrata de constitucionalidade do Ac. TC n.º 268/2022, disponível em: <http://www.tribunalconstitucional.pt>. Esta situação leva, nomeadamente, à definição de perfis (art. 4.º, n.º 4 do RGPD).

²³ Veja-se DIMITRI TOKMETZIS, *How your innocent smartphone passes on almost your entire life to the secret service*, 2014, disponível em: https://netzpolitik.org/wp-upload/bits_of_freedom_on_the_metadata_of_your_phone.pdf.

2. Evolução legislativa até à Lei do Cibercrime

Em 1987, embora não existisse uma previsão legal, os fornecedores de serviços já conservavam dados de base e dados de tráfego, pois a fatura do telefone dependia do tipo e duração das chamadas realizadas.

Posteriormente, foi emitido um parecer pela PGR²⁴, nos termos do qual a obtenção dos dados de tráfego dependia de decisão judicial. O fundamento para a sua obtenção resultava da conjugação dos arts. 187.º, 190.º e 269.º, n.º 1, al. c) do CPP previstos no âmbito das escutas telefónicas, aplicáveis por extensão²⁵. Quanto à conservação dos dados, não havia um regime legal expresso²⁶.

Após os atentados terroristas de 2001, 2004 e 2005, vários EM adotaram legislação destinada à conservação de metadados por parte dos fornecedores de serviços para fins de prevenção e repressão de infrações penais²⁷.

Em Portugal, a Diretiva 2002/58/CE foi transposta pela Lei n.º 41/2004, definindo-se, pela primeira vez, um regime específico sobre o tratamento de dados pessoais no âmbito da prestação de serviços de comunicações eletrónicas. Esta Lei passou a ser invocada como fundamento para a conservação, tendo-se mantido os fundamentos do CPP quanto ao acesso²⁸.

Com a revisão introduzida pela Lei n.º 48/2007, foi adotada no CPP uma norma específica sobre a utilização probatória dos metadados em processo judicial – art. 189.º, n.º 2 – passando esta a ser o fundamento para o acesso e utilização dos dados de tráfego e de localização²⁹.

²⁴ Parecer da PGR n.º 16/1994, disponível em: <https://www.ministeriopublico.pt/pareceres-pgr>.

²⁵ Veja-se os Acs. TRL de 10/12/2003, Proc. n.º 8673/2003-3 e de 23/06/2004, Proc. n.º 5845/2004-3, disponíveis em: <http://www.dgsi.pt>.

²⁶ RUI CARDOSO, “A conservação (...)”, cit., p. 42.

²⁷ Caso do Reino Unido, França, Irlanda e Itália. – cfr. DAVID SILVA RAMALHO, JOSÉ DUARTE COIMBRA, “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*, Ano 147.º (2015) IV, Coimbra, Almedina, p. 1005.

²⁸ Veja-se o Ac. TRG de 10/01/2005, Proc. n.º 2013/04-I e Ac. TRC de 17/05/2006, Proc. n.º 1265/06, disponíveis em: <http://www.dgsi.pt>. A conformidade constitucional desta interpretação foi suscitada ao TC, que concluiu que o art. 187.º, n.º 1 do CPP, “ao permitir a interceção e gravação das conversações ou comunicações telefónicas, permite também, inevitavelmente, o acesso a todos os dados de tráfego (...)”. – Ac. TC n.º 486/09, Proc. n.º 4/09, 2.4, disponível em: <http://www.tribunalconstitucional.pt>.

²⁹ No sentido de que a este regime estão sujeitos tanto os dados de localização conexos com comunicações, como aqueles independentes de uma comunicação, veja-se TIAGO CAIADO MILHEIRO, “Artigo 189.º”, cit., pp. 829 e 830.

A obtenção de dados de base não era abrangida por este regime, podendo ser levada a cabo pelo MP, de acordo com o art. 267.º do CPP, sendo, contudo, de obedecer ao segredo profissional (art. 135.º do CPP).

De seguida, surgiu a Lei n.º 32/2008, que transpôs a Diretiva 2006/24/CE, criada com o objetivo de harmonizar a legislação dos diversos EM³⁰. Contudo, esta Lei foi para além do escopo da Diretiva, uma vez que, além de regular a conservação dos metadados, prescreveu também sobre o regime de acesso (art. 9.º da Lei n.º 32/2008).

O regime da Lei n.º 32/2008 mostrou-se verdadeiramente distinto do que constava do art. 189.º, n.º 2 do CPP, criando problemas interpretativos.

Uma das principais diferenças disse respeito ao catálogo de crimes: ao definir *crime grave* na al. g) do n.º 1 do art. 2.º da Lei n.º 32/2008, o legislador deixou de fora alguns dos crimes do catálogo presente no n.º 1 do art. 187.º do CPP³¹.

Além disto, o regime da Lei n.º 32/2008 fez depender de prévia autorização do JIC não apenas a obtenção de dados de tráfego³², como também a obtenção de dados de base (arts. 4.º e 9.º da Lei n.º 32/2008).

O acesso aos metadados foi, ainda, restringido à fase de inquérito (art. 9.º, n.º 2 da Lei n.º 32/2008), requisito inexistente no CPP.

Colocou-se, assim, a questão de saber se o art. 189.º, n.º 2 do CPP tinha sido ou não revogado ou derogado pelo regime da Lei n.º 32/2008.

Na esteira de DUARTE RODRIGUES NUNES³³ e RITA CASTANHEIRA NEVES³⁴, o art. 9.º da Lei n.º 32/2008 derogou o art. 189.º, n.º 2 do CPP, permanecendo este em vigor nas situações em que estivessem em causa os crimes do catálogo do art. 187.º, n.º 1 do CPP não incluídos no art. 2.º, n.º 1, al. g) da Lei n.º 32/2008. Neste caso, os dados seriam conservados ao abrigo da Lei n.º 41/2004³⁵.

³⁰ Isto porque, os EM, ao abrigo do art. 15.º da Diretiva de 2002, adotaram medidas de conservação de dados significativamente diferentes entre si.

³¹ Aplicável por força do art. 189.º, n.º 2 do CPP.

³² Solução já prevista no CPP.

³³ DUARTE RODRIGUES NUNES, *O problema de admissibilidade dos métodos “ocultos” de investigação criminal como instrumento de resposta à criminalidade organizada*, Coimbra, Gestlegal, 2020, p. 565.

³⁴ RITA CASTANHEIRA NEVES, *As ingerências nas comunicações eletrónicas em processo penal*, Coimbra, Coimbra Editora 2011, p. 233.

³⁵ Neste sentido, veja-se o Ac. TRE de 28/02/2012, Proc. n.º 15/11.3JALRA-B.E1 e Ac. TRC de 01/06/2022, Proc. n.º 152/21.6GGCBR-A.C1, disponíveis em: <http://www.dgsi.pt>.

Contrariamente, houve quem entendesse que o art. 189.º, n.º 2 do CPP passou a aplicar-se apenas à obtenção de metadados em tempo real, ou seja, à sua interceção³⁶. O CPP não seria aplicável à obtenção de dados de comunicações já ocorridas, sendo de aplicar exclusivamente a Lei n.º 32/2008.

Ora, se é manifesto que o legislador optou por definir expressamente *crime grave*³⁷, exigindo, à primeira vista, que o art. 189.º, n.º 2 do CPP apresentasse um novo campo de aplicação, também não deixa de ser verdade que este artigo não sofreu qualquer alteração.

Por isto, consideramos dificilmente sustentável a opinião de que o art. 189.º, n.º 2 do CPP passou a ser aplicável apenas à obtenção de metadados em tempo real. Não era este o seu objeto antes da Lei n.º 32/2008, não se tendo verificado qualquer alteração que levasse a essa conclusão³⁸.

Não conseguimos conceber que a não menção no art. 189.º, n.º 2 do CPP ao regime dos arts. 187.º (n.ºs 2, 3, 5 a 8) e 188.º não deve ser interpretada como uma vontade de excluí-lo³⁹. A intenção do legislador⁴⁰ nunca foi que a norma se aplicasse à interceção de metadados, razão pela qual apenas existe uma menção expressa ao regime dos n.ºs 1 e 4 do art. 187.º.

Desta forma, apesar das eventuais incoerências que podem daqui advir, consideramos a Lei n.º 32/2008 um regime especial face ao regime geral presente no CPP, não apresentando, por isso, qualquer incompatibilidade com este último⁴¹.

Por fim, foi adotada a LC (Lei n.º 109/2009). Esta, regulando o domínio do cibercrime e da recolha de prova em suporte eletrónico, suscitou igualmente dúvidas quanto à sua compatibilidade com as normas já existentes – as da Lei n.º 32/2008 e as dos arts. 187.º e 189.º do CPP.

³⁶ Neste sentido, TIAGO CAIADO MILHEIRO, “Artigo 189.º”, cit., pp. 828 e 829 e Ac. TRL de 03/05/2016, Proc. n.º 73/16.4PFCSC-A.L1-5, Ac. TRE de 20/01/2015, Proc. n.º 648/14.6GCFAR-A.E1 e Ac. TRC de 23/11/2022, Proc. n.º 141/22.3GCLRA-A.CI, disponíveis em: <http://www.dgsi.pt>.

³⁷ Opção profundamente criticável, não incluindo os crimes de injúria, ameaça, coação e devassa da vida privada cometidos através de telefone. – Neste sentido, RITA CASTANHEIRA NEVES, *As ingerências (...)*, cit., pp. 232 e 233 e BENJAMIM SILVA RODRIGUES, *Da Prova Penal*, Tomo II, 1.ª Ed., Lisboa, Rei dos Livros, 2010, p. 421.

³⁸ Neste sentido, RUI CARDOSO, “*A conservação (...)*”, cit., pp. 44 a 47.

³⁹ Assim, TIAGO CAIADO MILHEIRO, “Artigo 189.º”, cit., p. 829.

⁴⁰ Atente-se à Exposição de Motivos da Proposta de Lei n.º 109/X (que esteve na origem da Lei n.º 48/2007), disponível em: <https://www.parlamento.pt>.

⁴¹ Veja-se a posição do Conselho Superior da Magistratura no preâmbulo da Portaria n.º 694/2010, disponível em: <https://www.pgdlisboa.pt/home.php> e a Nota Prática da PGR n.º 8/2016, disponível em: <https://cibercrime.ministeriopublico.pt/notas-praticas>.

De acordo com uma perspetiva, o art. 9.º da Lei n.º 32/2008 foi tacitamente revogado pelos arts. 12.º e ss. da LC⁴². Neste sentido, não sendo possível a harmonização destes dois sistemas, o art. 11.º, n.º 2 da LC deveria ser alvo de uma interpretação corretiva.

Contudo, segundo a doutrina e jurisprudência maioritárias, o art. 9.º da Lei n.º 32/2008 manteve-se em vigor, prevalecendo sobre os arts. 12.º e ss. da LC⁴³.

Esta orientação, que consideramos a mais adequada, apoia-se sobretudo no art. 11.º, n.º 2 da LC, que ressalva expressamente o regime da Lei n.º 32/2008. Assim, sustenta-se que as áreas de aplicação são diferentes: o regime da LC é aplicável aos crimes previstos no seu art. 11.º, n.º 1 e a Lei n.º 32/2008 aplica-se à investigação de crimes graves, conforme definido no seu art. 2.º, n.º 1, al. g)⁴⁴.

A LC “não contém qualquer norma que seja fundamento para a conservação de dados”⁴⁵, sendo importante precisar a diferença entre a conservação genérica de dados (art. 4.º da Lei n.º 32/2008) e a preservação de dados (*quick freeze* – art. 12.º da LC).

Por um lado, a conservação de dados exige que os operadores retenham os dados de todos os utilizadores dos serviços de comunicações, para poderem ser acedidos pelas autoridades competentes para fins de prevenção, deteção e repressão criminal.

Já a preservação de dados ocorre nos casos em que se exige a uma pessoa ou entidade que preserve dados informáticos específicos, impedindo a sua perda ou

⁴² Neste sentido, DUARTE RODRIGUES NUNES, *Os meios (...)*, cit., p. 25, PAULO DÁ MESQUITA, “Prolegómeno sobre prova eletrónica e interceção de telecomunicações no direito processual penal português – o Código e a Lei do Cibercrime”, in *Processo Penal, Prova e Sistema Judiciário*, 1.ª ed., Coimbra, Coimbra Editora, 2010, p. 111 e Ac. TRL de 22/01/2013, Proc. n.º 581/12.6PLSNT-A.L1-501, Ac. TRC de 26/02/2014, Proc. n.º 559/12.0GBOBR-A.C1 e Ac. TRE de 20/01/2015, Proc. n.º 648/14.6GCFAR-A.E1, disponíveis em: <http://www.dgsi.pt>.

⁴³ Neste sentido, PAULO PINTO DE ALBUQUERQUE, *Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, 3.ª ed., Lisboa, Universidade Católica, 2008, p. 549, PEDRO DIAS VENÂNCIO, *Lei do Cibercrime*, Coimbra, Coimbra Editora, 2011, pp. 100 e 101, BENJAMIM SILVA RODRIGUES, *Da Prova (...)*, cit., pp. 439 e 440, CARLOS PINHO, “Os problemas interpretativos resultantes da Lei n.º 32/2008, de 17 de Julho”, in *Revista do Ministério Público*, n.º 129, jan.-mar. 2012, p. 79, RITA CASTANHEIRA NEVES, *As ingerências (...)*, cit., p. 237, TIAGO CAIADO MILHEIRO, “Artigo 189.º”, cit., p. 833 e Ac. TRL de 03/05/2016, Proc. n.º 73/16.4PFCSC-A.L1-5, Ac. TRE de 14/07/2020, Proc. n.º 9/20.8GAMTL-A.E1 e Ac. TRC de 12/10/2022, Proc. n.º 538/22.9JALRA.C1, disponíveis em: <http://www.dgsi.pt>.

⁴⁴ Neste âmbito, “pensa-se que o legislador quis prever e regulamentar diferentemente o acesso e obtenção de dados informáticos como pressuposto geral a todos os crimes ditos informáticos (...) porque a sua prova só é praticamente possível através da recolha de prova em suporte eletrónico, consagrando-se aqui requisitos mais flexíveis de admissibilidade.” – cfr. RITA CASTANHEIRA NEVES, *As ingerências (...)*, cit., pp. 237 e 238. Atenda-se, aqui, ao art. 12.º da LC.

⁴⁵ RUI CARDOSO, “*A conservação (...)*”, cit., p. 48.

modificação, por um determinado período. Tal ordem tem o prazo de três meses, passível de ser alargado (art. 12.º, n.º 3, al. c) e 5 da LC)⁴⁶.

O art. 14.º da LC, referente à injunção para apresentação ou concessão do acesso a dados, nada alterou quanto ao regime de dados de tráfego⁴⁷. De facto, segundo o seu n.º 4, este meio processual não pode ser utilizado para a recolha de dados de tráfego (ou de conteúdo).

Importa ainda fazer alusão ao art. 18.º da LC, que, regulando a interceção e gravação de dados em transmissão, não se aplica a dados armazenados. O seu n.º 4 remete para o regime dos arts. 187.º, 188.º e 190.º do CPP. Nenhuma referência é feita ao art. 189.º do CPP, evidenciando, mais uma vez, que este apenas se aplica à obtenção de dados de tráfego armazenados⁴⁸.

Neste contexto, alerta-se para o facto de “as insuficiências da Lei n.º 32/2008 não terem sido supridas pelo artigo 18.º da Lei n.º 109/2009”, uma vez que este, ao remeter para o art. 187.º do CPP, não permite que o recurso a este meio processual para “prova de crimes de ameaças e injúrias cometidas pelo correio eletrónico e ainda dos crimes de dano informático, acesso ilegítimo, interceção ilegítima e reprodução ilegítima de programa protegido”⁴⁹.

Posto isto, tanto a Lei n.º 32/2008, como a LC, enquanto leis extravagantes, reduziram, significativamente, o âmbito de aplicação inicial do art. 189.º do CPP⁵⁰.

Verifica-se, aqui, uma sobreposição de regras relativamente ao mesmo objeto, que resulta numa grande incerteza jurídica e coloca em causa a investigação de crimes de grande impacto social, atendendo às várias interpretações doutrinárias e jurisprudenciais que tem suscitado⁵¹.

Impunha-se, assim, a integração das regras no CPP enquanto “diploma estruturante”, sendo esta a “opção mais coerente com a tradição portuguesa”⁵².

⁴⁶ A propósito desta diferenciação, veja-se CARLOS PINHO, “Lei de retenção de dados de comunicações eletrónicas: aposentar ou reformar?”, in *Revista do Ministério Público*, n.º 154, abr.-jun. 2018, pp. 179 a 185.

⁴⁷ Apenas quanto aos dados de base.

⁴⁸ Neste sentido, RUI CARDOSO, “A conservação (...)”, cit., p. 56.

⁴⁹ PAULO PINTO DE ALBUQUERQUE, *Comentário (...)*, cit. p. 549.

⁵⁰ JOÃO CONDE CORREIA, “Prova Digital (...)”, cit., p. 36.

⁵¹ Veja-se o Ac. TRC de 01/06/2022, Proc. n.º 152/21.6GGCBR-A.C1, disponível em: <http://www.dgsi.pt>;

⁵² PAULO DÁ MESQUITA, “Prolegómeno (...)”, cit., p. 101. No mesmo sentido, RUI CARDOSO, “A conservação (...)”, cit., p. 46.

Capítulo II – Da jurisprudência do TJUE

1. O Acórdão *Digital Rights Ireland*

A Diretiva 2006/24/CE alterou a Diretiva 2002/58/CE. Ao consagrar uma obrigação de conservação de metadados no art. 3.º, derogou, nomeadamente, os arts. 5.º, 6.º e 9.º desta última Diretiva, que continham um conjunto de garantias de proteção dos direitos fundamentais consagrados nos arts. 7.º e 8.º da CDFUE.

Além disto, foi excluída a aplicabilidade do n.º 1 do art. 15.º da Diretiva 2002/58/CE aos dados conservados ao abrigo da Diretiva 2006/24/CE, conforme previsto no seu art. 11.º.

No âmbito do Ac. de 8 de abril 2014, conhecido como *Digital Rights Ireland*⁵³, o TJUE foi instado a pronunciar-se sobre a questão de saber se a Diretiva 2006/24/CE era válida ao abrigo, nomeadamente, dos arts. 7.º, 8.º e 11.º da CDFUE, tendo concluído pela sua invalidade.

Começando por considerar que a obrigação de conservação de dados prevista no art. 3.º da Diretiva era abrangida pelo âmbito de aplicação dos arts. 7.º e 8.º da CDFUE⁵⁴, o TJUE entendeu que a mesma comportava uma ingerência nos direitos fundamentais aí previstos, concentrando-se na análise da sua legitimidade, nos termos do art. 52.º, n.º 1 da CDFUE⁵⁵.

Apesar de concluir que o conteúdo essencial dos direitos fundamentais não era afetado⁵⁶ e que o subprincípio da adequação se encontrava preenchido⁵⁷, o mesmo não se verificou quanto ao subprincípio da necessidade, na medida em que: i) a Diretiva abrangia “todos os assinantes e utilizadores registados”, não se limitando 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 (...)”⁵⁸; ii) quanto ao acesso, não eram estabelecidos critérios objetivos que permitissem “limitar o número de pessoas com autorização de acesso e de

⁵³ Ac. *Digital Rights Ireland*, de 08/04/2014, Procs. C-293/12 (*Hight Court* irlandês) e C-594/12 (*Verfassungsgerichtshof* austríaco), disponível em: https://curia.europa.eu/jcms/jcms/j_6/pt/.

⁵⁴ *Ibidem*, §29. O direito fundamental à proteção de dados pessoais, presente no art. 8.º da CDFUE, está “indissociavelmente relacionado com o direito ao respeito da vida privada” consagrado no art. 7.º da CDFUE – cfr. Ac. *Volker und Markus Schecke*, de 09/11/2010, Procs. C-92/09 e C-93/09, §47, disponível em: https://curia.europa.eu/jcms/jcms/j_6/pt/.

⁵⁵ Ac. *Digital Rights Ireland*, §§37 e 38.

⁵⁶ *Ibidem*, §§39 e 40.

⁵⁷ *Ibidem*, §49.

⁵⁸ *Ibidem*, §59.

utilização posterior dos dados conservados ao estritamente necessário à luz do objetivo prosseguido”⁵⁹; iii) relativamente à duração da conservação, a sua determinação dever-se-ia basear em “critérios objetivos”, criticando-se o facto de não se distinguir entre as categorias de dados presentes no art. 5.⁶⁰.

Além disto, alertou-se para o facto de a Diretiva não impor que os dados sejam conservados no território da UE, não estando garantida a fiscalização por uma entidade independente (art. 8.º, n.º 3 da CDFUE)⁶¹ e sublinhou-se que a falta de notificação do acesso pode criar no titular dos dados a sensação de que a sua vida privada é “constantemente vigiada”⁶².

Não obstante terem ficado por determinar os efeitos concretos desta declaração⁶³, sendo os EM os destinatários da Diretiva, foi ao nível dos efeitos da declaração de invalidade em relação às medidas legislativas nacionais que se colocaram as principais questões.

Primeiramente, o TJUE não tem poderes de cognição sobre atos de direito nacional. O DUE conserva autonomia face à ordem jurídica interna, pelo que a declaração de invalidade da Diretiva não implica diretamente a invalidade da lei nacional que a transponha. Contudo, sendo aprovada em aplicação do DUE, esta última terá, igualmente, de ser confrontada com a CDFUE (art. 51.º), em especial com os seus arts. 7.º, 8.º e 52.º, n.º 1⁶⁴. A relação de contrariedade que daí possa advir implica não a invalidade, mas a inaplicabilidade do ato nacional. É este o sentido do princípio do primado do DUE.

⁵⁹ *Ibidem*, §62.

⁶⁰ *Ibidem*, §§63 e 64.

⁶¹ *Ibidem*, §68.

⁶² *Ibidem*, §37.

⁶³ Quanto ao alcance material, perante o DUE globalmente considerado, razões de uniformidade impõem que a inaplicabilidade da Diretiva seja um efeito de ordem genérica. – Neste sentido, DAVID SILVA RAMALHO, JOSÉ DUARTE COIMBRA, “A declaração (...)”, cit., pp. 1019-1022 e ALESSANDRA SILVEIRA, PEDRO MIGUEL FREITAS, “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*, n.º 1, vol. 9, Brasília, Universidade de Brasília, 2017, p. 52. Contra, JOÃO CONDE CORREIA, “Prova Digital (...)”, cit., p. 38. Relativamente à eficácia temporal, a declaração de invalidade produz efeitos retroativos (*ex tunc*), salvo se o Tribunal limitar temporalmente os efeitos do Ac. por razões de segurança jurídica. – cfr. Ac. *Roquette Frères*, de 15/10/1980, Proc. C-145/79, §§50 a 53, disponível em: https://curia.europa.eu/jcms/jcms/j_6/pt/ e Comunicado de Imprensa n.º 54/14, de 08/04/2014, relativo ao Ac. *Digital Rights Ireland*, disponível em: https://curia.europa.eu/jcms/jcms/j_6/pt/.

⁶⁴ Neste sentido, CLARA GUERRA, FILIPA GALVÃO, “Anotação ao Acórdão do Tribunal de Justiça (Grande Secção) de 8 de abril de 2014”, in *Forum de proteção de dados*, n.º 1, jul. 2015, p. 77; DAVID SILVA RAMALHO, JOSÉ DUARTE COIMBRA, “A declaração (...)”, cit., pp. 1028 e 1029 e Deliberações CNPD n.º 641/2007 e n.º 1008/2017, disponíveis em: <https://www.cnpd.pt/>;

Atendendo a isto, a reação dos EM não foi consensual, tendo apenas dez declarado inválidas as leis nacionais que transpunham a Diretiva⁶⁵. Nos restantes 16 EM, assumiram-se duas posições distintas, tendo uns sustentado que a validade formal das suas leis não foi posta em causa e outros que as exigências substanciais da decisão do TJUE estavam previamente satisfeitas⁶⁶. Este foi o caso de Portugal, onde a validade da Lei n.º 32/2008 não foi posta em causa⁶⁷. De facto, entendeu-se que esta, uma vez que ia para além das exigências da Diretiva, escapava à generalidade das críticas formuladas pelo TJUE⁶⁸.

A nosso ver, só se consegue sustentar um juízo igualmente negativo quanto à Lei n.º 32/2008 se as objeções a respeito da Diretiva forem consideradas individualmente. Queremos com isto dizer que, não tendo o TJUE mencionado expressamente que a mera conservação generalizada e indiferenciada de dados excedia o estritamente necessário⁶⁹, a conjugação desta com regras de segurança⁷⁰ e de acesso estritas, nos termos previstos na lei nacional, faz da mesma um regime substancialmente mais rigoroso, quando comparado com a Diretiva de 2006.

⁶⁵ Caso a Áustria, Bélgica, Eslováquia e Eslovénia – cfr. ALESSANDRA SILVEIRA, PEDRO MIGUEL FREITAS, “Implicações da (...)”, cit., p. 57.

⁶⁶ Nota Prática da PGR n.º 7/2015, disponível em: <https://cibercrime.ministeriopublico.pt/notas-praticas>.

⁶⁷ Até ao Ac. do TC n.º 268/2022, os tribunais portugueses continuaram a recorrer à Lei n.º 32/2008, não se pronunciando sobre o impacto do Ac. *Digital Rights Ireland*. – veja-se os Acs. TRE de 06/01/2015, Proc. n.º 6793/11.2TDLSB-A.E1 e de 19/05/2015, Proc. n.º 54/15.5GCBNV-A.E1, Ac. TRP de 07/07/2016, Proc. n.º 2039/14.0JAPRT.P1, Ac. TRC de 08/11/2017, Proc. n.º 380/17.9JACBR.C1 e Ac. TRL de 28/11/2018, Proc. n.º 8617/17.8T9LSB-A.L1-3, disponíveis em <http://www.dgsi.pt>.

⁶⁸ Como referido *supra*, a Lei n.º 32/2008 estipulou condições de acesso aos dados (art. 9.º) e definiu o conceito de *crime grave* (art. 2.º, n.º 1, al. g)), estabelecendo, ainda, particulares deveres de proteção e segurança dos dados (art. 7.º). Contudo, no sentido de revisão da Lei n.º 32/2008, veja-se o Ac. TRE de 22/02/2022, Proc. n.º 188/21.7GAVNO.E1, disponível em <http://www.dgsi.pt>.

⁶⁹ Criando, compreensivelmente, em alguns, a convicção de que a existência de regras de acesso estritas compensa a conservação generalizada de dados. – cfr. IAIN CAMERON, “*A. Court of Justice Balancing data protection and law enforcement needs: Tele2 Sverige and Watson*”, in *Common Market Law Review*, 54, *Kluwer Law International*, Reino Unido, 2017, p. 1470 e TUOMAS OJANEN, “*Privacy Is More Than Just a Seven-Letter Word: The Court of Justice of the European Union Sets Constitutional Limits on Mass Surveillance*”, in *European Constitutional Law Review*, 10, *Cambridge University Press*, Reino Unido, 2014.

⁷⁰ Atenda-se ao art. 7.º, n.º 5 da Lei n.º 32/2008: ao sujeitar a conservação dos dados ao controlo da CNPD, está implicitamente a impor que os dados têm de ser armazenados no território português. – Neste sentido, declaração de voto de LINO RIBEIRO ao Ac. TC n.º 268/2022, Proc. n.º 828/2019, disponível em: <http://www.tribunalconstitucional.pt> e DUARTE RODRIGUES NUNES, “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 do Ministério Público*, n.º 170, abr.-jun. 2022, p. 40.

2. A posterior reorientação da posição do TJUE

Após a declaração de invalidade da Diretiva, o TJUE voltou a pronunciar-se sobre esta matéria, incidindo agora sobre a interpretação do art. 15.º, n.º 1 da Diretiva 2002/58/CE.

No Ac. *Tele 2*⁷¹, o TJUE parece ter redirecionado a jurisprudência anterior, tendo-se pronunciado expressamente no sentido de a conservação generalizada e indiscriminada dos dados de tráfego e de localização exceder o estritamente necessário⁷².

Ademais, procurou desenvolver os elementos objetivos que devem presidir à conservação seletiva dos mesmos, estabelecendo que o critério geográfico deve respeitar às situações em que as autoridades nacionais considerem, objetivamente, que existe um risco elevado de preparação ou de execução de atos de criminalidade grave, numa zona geográfica⁷³.

Quanto ao acesso, o Tribunal determinou a necessidade da notificação do mesmo aos titulares dos dados para efeitos de eventual exercício do direito de recurso⁷⁴.

Mais tarde, a 6 de outubro de 2020⁷⁵, 5 de abril de 2022⁷⁶ e 20 de setembro de 2022⁷⁷, o TJUE seguiu a mesma linha de entendimento, embora tenha feito uma abordagem mais exaustiva quanto à questão da conservação de metadados.

O Tribunal estabeleceu, inevitavelmente, exceções à regra segundo a qual os dados de tráfego e de localização não podem ser conservados de forma geral e indiscriminada.

Desta forma, determinou-se que, para efeitos da salvaguarda da segurança nacional, o art. 15.º, n.º 1 da Diretiva 2002/58/CE, lido à luz dos arts. 7.º, 8.º, 11.º e 52.º, n.º 1 da CDFUE, não se opõe a medidas legislativas que imponham aos prestadores de serviços uma conservação generalizada e indiferenciada de dados de tráfego e de localização, mas apenas se: i) existirem indícios concretos de uma ameaça real e atual ou

⁷¹ Ac. *Tele 2*, de 21/12/2016, Procs. C-203/15 (*Kammarrätten i Stockholm*) e C-698/15 (*Court of Appeal - England & Wales*), disponível em: https://curia.europa.eu/jcms/jcms/j_6/pt/. Neste Ac., o TJUE considera, igualmente, como parâmetro interpretativo o direito fundamental à expressão (art. 11.º da CDFUE), além dos direitos consagrados nos arts. 7.º e 8.º da CDFUE, orientação mantida nos Acs. posteriores.

⁷² *Ibidem*, §107.

⁷³ *Ibidem*, §111.

⁷⁴ *Ibidem*, §121.

⁷⁵ Ac. *La Quadrature du Net*, de 06/10/2020, Procs. C- 511/18 e C-512/18 (*Conseil d'État*) e C-520/18 (*Cour constitutionnelle*), disponível em: https://curia.europa.eu/jcms/jcms/j_6/pt/.

⁷⁶ Ac. *Commissioner of An Garda Síochána*, de 05/04/2022, Proc. C-140/20 (*Supreme Court*), disponível em: https://curia.europa.eu/jcms/jcms/j_6/pt/.

⁷⁷ Ac. *SpaceNet*, de 20/09/2022, Procs. C-793/19 (*Bundesverwaltungsgericht*) e C-794/19 (*Bundesverwaltungsgericht*), disponível em: https://curia.europa.eu/jcms/jcms/j_6/pt/.

previsível para a segurança nacional; ii) for definido um prazo de conservação, renovável (de forma não sistemática) em caso de persistência da ameaça e iii) a decisão que impõe a conservação seja objeto de fiscalização concreta por um tribunal ou uma entidade administrativa independente⁷⁸.

Além disto, o TJUE estipulou que, para efeitos tanto de salvaguarda da segurança nacional, como de luta contra a criminalidade grave e de prevenção de ameaças graves contra a segurança pública, o art. 15.º, n.º 1 da Diretiva 2002/58/CE, lido à luz dos arts. 7.º, 8.º, 11.º e 52.º, n.º 1 da CDFUE, não se opõe a medidas legislativas que imponham aos prestadores de serviços: i) uma conservação seletiva dos dados de tráfego e de localização, com base em critérios objetivos e por um período limitado ao estritamente necessário, embora renovável⁷⁹; ii) uma conservação generalizada e indiferenciada dos endereços IP atribuídos à fonte de uma ligação, por um período limitado ao estritamente necessário⁸⁰ e/ou iii) uma conservação generalizada e indiferenciada de dados relativos à identidade civil dos utilizadores⁸¹.

Por fim, concluiu-se que, para efeitos da luta contra a criminalidade grave e, *a fortiori*, da salvaguarda da segurança nacional, uma medida que imponha, por um determinado período, a conservação rápida de dados de tráfego e de localização, através de uma decisão sujeita a fiscalização jurisdicional efetiva, é admitida ao abrigo do art. 15.º, n.º 1 da Diretiva 2002/58/CE, lido à luz dos arts. 7.º, 8.º, 11.º e 52.º, n.º 1 da CDFUE⁸².

Quanto ao acesso, releva o entendimento do TJUE no *Ac. Ministerio Fiscal*⁸³ e no *Ac. Prokuratuur*⁸⁴.

Tendo o TJUE adotado uma atitude mais realista à luta contra a criminalidade grave, é importante precisar alguns pontos.

⁷⁸ *Ac. La Quadrature du Net*, §§134 a 139 e 229, *Ac. Commissioner of An Garda Síochána*, §§58 a 62 e *Ac. SpaceNet*, §§72, 92 a 94 e 131.

⁷⁹ *Ac. La Quadrature du Net*, §§140 a 151 e 229, *Ac. Commissioner of An Garda Síochána*, §§76 a 84, e *Ac. SpaceNet*, §§105 a 113 e 131.

⁸⁰ *Ac. La Quadrature du Net*, §§152 a 156 e 229, *Ac. Commissioner of An Garda Síochána*, §§73 e 74, *Ac. SpaceNet*, §§100 a 103 e 131.

⁸¹ *Ac. La Quadrature du Net*, §§157 a 159, *Ac. Commissioner of An Garda Síochána*, §§70 a 72 *Ac. SpaceNet*, §§ 97 a 99 e 131.

⁸² *Ac. La Quadrature du Net*, §§160 a 167, *Ac. Commissioner of An Garda Síochána*, §§85 a 91 e *Ac. SpaceNet*, §§114 a 120 e 131.

⁸³ *Ac. Ministerio Fiscal*, de 02/10/2018, Proc. C-207/16 (*Audiencia Provincial de Tarragona*), §63, disponível em: https://curia.europa.eu/jcms/jcms/j_6/pt/.

⁸⁴ *Ac. Prokuratuur*, de 02/03/2021, Proc. C-746/18 (*Riigikohus*), §§45 e 59, disponível em: https://curia.europa.eu/jcms/jcms/j_6/pt/.

O primeiro respeita à relação entre a conservação e o acesso aos dados de tráfego e de localização, relativamente à qual o TJUE parece ter reorientado o seu entendimento. De facto, apesar de, no Ac. *Digital Rights*, o Tribunal não considerar a conservação indiscriminada dos dados uma medida, por si só, excessiva, nos Acs. posteriores, já o entende, analisando, de forma separada, a ingerência nos direitos fundamentais resultante da conservação e do acesso⁸⁵⁻⁸⁶.

Quanto aos critérios de seleção a adotar pelos EM, o TJUE explicitou a sua posição.

Relativamente à conservação de metadados em função das categorias de pessoas em causa, esta pode dirigir-se contra pessoas “objeto de um inquérito ou de outras medidas de vigilância atuais ou de inscrição no registo criminal nacional que mencione uma condenação anterior por atos de criminalidade grave que possam implicar um risco elevado de reincidência”⁸⁷.

Quanto ao critério geográfico, o TJUE determinou que as zonas a ser consideradas pelas autoridades nacionais competentes podem ser “(...) locais caracterizados por um elevado número de atos de criminalidade grave, locais particularmente expostos à prática de atos de criminalidade grave, tais como locais ou infraestruturas frequentadas regularmente por um número muito grande de pessoas, ou ainda locais estratégicos, como aeroportos, estações ou zonas de portagens.”⁸⁸. Estabeleceu-se, ainda, que este critério pode assentar na “taxa média de criminalidade numa zona geográfica”⁸⁹.

Sem mencionar quais, o TJUE admitiu, igualmente, a possibilidade de se recorrer a critérios de seleção para além do pessoal ou geográfico, desde que “objetivos e não discriminatórios”⁹⁰.

⁸⁵ Apesar do §79 do Ac. *Tele 2*.

⁸⁶ Ac. *SpaceNet*, §91.

⁸⁷ *Ibidem*, §107.

⁸⁸ Ac. *La Quadrature du Net*, §150.

⁸⁹ Ac. *SpaceNet*, §109.

⁹⁰ *Ibidem*, §112.

Capítulo III – Do impacto do DUE na ordem jurídica interna

1. O Acórdão do TC n.º 268/2022

Após vários anos de inércia e tendo a CNPD já se pronunciado no sentido de que a Lei n.º 32/2008 violava a CDFUE e a CRP⁹¹, o TC declarou a inconstitucionalidade daquela Lei no Ac. n.º 268/2022⁹², mais especificamente a conjugação dos seus arts. 4.º e 6.º e o seu art. 9.º.

Esta decisão foi suscitada pela Provedora de Justiça (art. 281.º, n.º 2, al. d) da CRP), tendo o TC começado por determinar que a conservação e o acesso aos metadados em causa, por serem “aptos a revelar aspetos relevantes da vida privada e familiar dos cidadãos”, implicam uma ingerência nos direitos à reserva da vida privada e ao livre desenvolvimento da personalidade (art. 26.º, n.º 1 da CRP) e no direito à autodeterminação informativa (art. 35.º, n.ºs 1 e 4 da CRP).

Quanto ao direito à inviolabilidade das comunicações (art. 34.º, n.ºs 1 e 4 da CRP), o TC entendeu que este apenas abrange os dados de tráfego “quando pressuponham uma comunicação entre pessoas”, excluindo, assim, os dados de base e os dados de tráfego gerados pela comunicação entre um sujeito e uma máquina⁹³.

Determinando que a relevância do DUE se cinge à interpretação que é feita da Constituição, nos termos do cânone da interpretação conforme⁹⁴⁻⁹⁵, o TC não adotou, todavia, a metodologia seguida pelo TJUE quanto à relação entre a conservação e o acesso aos metadados na análise do princípio de proporcionalidade.

Em vez de analisar separadamente estes dois momentos, o TC defendeu, devidamente, que “(...) do ponto de vista da proporcionalidade (...) não é indiferente a consideração das condições de análise, tratamento e transmissão às autoridades públicas

⁹¹ Deliberação CNPD n.º 1008/2017, disponível em: <https://www.cnpd.pt>. Nesta, a CNPD deliberou desaplicar a Lei n.º 32/2008 nas situações que lhe fossem submetidas para apreciação.

⁹² Ac. TC n.º 268/2022, Proc. n.º 828/2019, disponível em: <http://www.tribunalconstitucional.pt>.

⁹³ *Ibidem*, 10. O TC não invoca, contudo, quanto à conservação generalizada dos dados de tráfego, a restrição a este direito como fundamento da inconstitucionalidade das normas dos arts. 4.º e 6.º da Lei n.º 32/2008, o que foi criticado por alguns dos Conselheiros numa declaração de voto conjunta.

⁹⁴ Defendendo a interpretação dos parâmetros constitucionais mais próxima do direito europeu, de forma a garantir o efeito útil das normas europeias, nos termos do princípio da cooperação leal (art. 4.º, n.º 3 do TUE). – cfr. *Ibidem*, 8.2.

⁹⁵ Alguns Conselheiros discordaram desta posição, defendendo, na sua declaração de voto, a integração na apreciação da constitucionalidade do *standard europeu* de controlo de proporcionalidade, enquanto manifestação do princípio da cooperação leal.

dos dados conservados”⁹⁶. Contudo, já não acompanhamos o TC quando recorre a esta orientação apenas para fundamentar a não inconstitucionalidade do regime dos dados de base, desconsiderando-a em matéria de dados de tráfego⁹⁷.

Quanto à conservação dos dados de base, o TC seguiu o entendimento adotado no Ac. n.º 420/2017, nos termos do qual o regime da conservação do “nome e endereço do assinante ou do utilizador registado, a quem o endereço de protocolo IP está atribuído” é conforme à Constituição⁹⁸.

Nestes termos, analisando o princípio da proporcionalidade, o TC concluiu pelo preenchimento de todos os seus subprincípios: adequação⁹⁹, exigibilidade e proporcionalidade em sentido estrito. Defendeu, assim, a inexistência de medidas menos intrusivas com igual eficácia¹⁰⁰ e recorreu à decisão do TJUE de admissibilidade de conservação geral e indiscriminada dos endereços IP da fonte de comunicação, concluindo que, por maioria de razão, a “conservação de dados de base que *não pressupõem a análise de quaisquer comunicações* (números de telefone, endereços de correio eletrónico, etc.)” deve ser “igualmente conforme” ao art. 18.º, n.º 2 da CRP¹⁰¹.

Contudo, não tendo o legislador prescrito expressamente a necessidade de o armazenamento de dados ocorrer no território da UE, o TC decidiu declarar tal obrigação de conservação inconstitucional, por violação do direito à autodeterminação informativa (art. 35.º, n.ºs 1 e 4 da CRP), aplicando-se o mesmo à obrigação de conservação dos dados de tráfego e de localização.

Quanto a esta, outro fundamento concorreu para a declaração da sua inconstitucionalidade.

Embora não concebendo medidas com a mesma eficácia que a conservação indiscriminada de todos os dados, o TC concluiu que a ingerência nos direitos fundamentais à reserva da intimidade da vida privada (art. 26.º, n.º 1 da CRP) e à autodeterminação informativa (art. 35.º, n.º 1 da CRP) resultante dessa medida, no que concerne ao seu âmbito subjetivo (pessoal), não é compensada pelos efeitos positivos no

⁹⁶ *Ibidem*, 14. Entendimento já preconizado no Ac. do TC n.º 420/2017, Proc. n.º 917/16, disponível em: <http://www.tribunalconstitucional.pt> e adotado pelo TEDH no Ac. *Breyer*, de 30/01/2020, Proc. C-582/14, disponível em: <https://eur-lex.europa.eu/homepage.html>.

⁹⁷ Neste sentido, declaração de voto de LINO RIBEIRO ao Ac. TC n.º 268/2022, Proc. n.º 828/2019, disponível em: <http://www.tribunalconstitucional.pt>.

⁹⁸ Ac. TC n.º 420/2017, Proc. n.º 917/16, 14, disponível em: <http://www.tribunalconstitucional.pt>.

⁹⁹ Ac. TC n.º 268/2022, Proc. n.º 828/2019, 17.2, disponível em: <http://www.tribunalconstitucional.pt>.

¹⁰⁰ *Ibidem*, 17.3.

¹⁰¹ *Ibidem*.

combate à criminalidade, não estando preenchido o subprincípio de proporcionalidade em sentido estrito¹⁰².

Relativamente ao acesso, defendendo que a inexistência da notificação do acesso aos titulares dos dados restringe o direito à autodeterminação informativa (art. 35.º, n.º 1 da CRP) e o direito a uma tutela jurisdicional efetiva (art. 20.º, n.º 1 da CRP), o TC entendeu que o crivo da adequação não se encontra preenchido, por não se vislumbrar um “motivo constitucionalmente relevante que legitime a inexistência de uma notificação”¹⁰³. Assim, a norma do art. 9.º foi igualmente declarada inconstitucional nesta parte.

Como consequência, a Lei n.º 32/2008 deixou de poder constituir fundamento não só para a conservação de quaisquer metadados de telecomunicações (arts. 4.º e 6.º), mas também para a sua obtenção e utilização probatória (art. 9.º).

O TC não fixou os efeitos da inconstitucionalidade (art. 282.º, n.º 4 da CRP), pelo que, aplicando-se o regime regra, a declaração de inconstitucionalidade com força obrigatória geral produz efeitos desde a entrada em vigor da norma declarada inconstitucional (art. 282.º, n.º 1 da CRP).

Assim, várias decisões de tribunais ainda não transitadas em julgado foram anuladas, uma vez que a prova se baseava essencialmente em metadados¹⁰⁴.

Contudo, o entendimento que resultou deste Ac. não foi unânime: enquanto alguma jurisprudência determinou a possibilidade de aceder aos metadados conservados pelos fornecedores de serviços ao abrigo da Lei n.º 41/2004¹⁰⁵ para efeitos de prova em processo penal¹⁰⁶, houve quem entendesse que tal seria defraudar o âmbito de regulamentação dessa Lei, “deixando entrar pela janela” aquilo a que o TC “fechou a porta”¹⁰⁷.

A este respeito, não se tendo o TC pronunciado sobre a admissibilidade de conservação dos dados para fins de faturação, nem sobre a admissibilidade de posterior

¹⁰² Por isto, o TC não analisa os restantes elementos dos quais dependeria a proporcionalidade da medida, como o prazo e as condições de segurança do armazenamento.

¹⁰³ Ac. TC n.º 268/2022, Proc. n.º 828/2019, 19.2, disponível em: <http://www.tribunalconstitucional.pt>.

¹⁰⁴ Ac. TRL de 26/01/2023, Proc. n.º 849/20.8PBCSC.L1-9 e Ac. TRE de 28/02/2023 Proc. n.º 661/17.1TELSB.E1 (caso de Tancos), disponíveis em: <http://www.dgsi.pt>.

¹⁰⁵ Por um período de seis meses (art. 6.º, n.º 3 da Lei n.º 41/2004 e art. 10.º, n.º 1 da Lei n.º 23/96).

¹⁰⁶ Neste sentido, RUI CARDOSO, “A conservação (...)”, cit., p. 72 e Ac. TRG de 02/05/2023, Proc. n.º 12/23.6 PBGMR-A.G1 e Ac. TRC de 27/09/2023, Proc. n.º 13/20.6PEVIS.C1, disponíveis em: <http://www.dgsi.pt>.

¹⁰⁷ Veja-se o Ac. TRC de 12/10/2022, Proc. n.º 538/22.9JALRA.C1 e Acs. TRP de 07/12/2022, Proc. n.º 5011/22.2JAPRT-A.P1, de 18/01/2023, Proc. n.º 47/22.6PEPRT-P.P1, de 01/02/2023, Proc. n.º 2748/22.0JAPRT-A.P1, disponíveis em: <http://www.dgsi.pt>.

utilização probatória desses dados, concluímos pela possibilidade de acesso aos mesmos pelas autoridades competentes¹⁰⁸. Se assim não fosse, seria inaceitável permitir-se às operadoras de comunicações a conservação e utilização dos dados para efeitos de faturação e não permitir o mesmo para a prova de crimes graves¹⁰⁹.

Relativamente aos casos transitados em julgado (art. 282.º, n.º 3 da CRP), o TC nada precisou¹¹⁰, o que levantou dúvidas quanto à extensão da sua decisão aos mesmos, colocando a hipótese de recorrer à al. f) do n.º 1 do art. 449.º do CPP.

Conforme o princípio de hierarquia de normas, o CPP tem de ser interpretado conforme a CRP, pelo que o pedido de revisão de sentença só pode ter como fundamento a declaração de inconstitucionalidade com força obrigatória geral nos casos em que o TC determine a reabertura do caso julgado. Assim, nada tendo o TC dito, consideramos que a sua decisão em nada afeta os casos julgados¹¹¹.

2. Após a declaração de inconstitucionalidade do cerne da Lei n.º 32/2008

O Ac. do TC n.º 268/2022 conduziu a um novo processo legislativo.

Enquanto os partidos optaram por propor alterações à Lei de 2008¹¹², o Governo optou pela sua revogação¹¹³, propondo a utilização pelas autoridades judiciárias dos dados conservados pelas empresas de telecomunicações para efeitos de faturação, nos termos do n.º 2 do art. 6.º da Lei n.º 41/2004.

¹⁰⁸ Nos termos do art. 14.º, n.º 4, al. b) da LC ou do art. 189.º, n.º 2 do CPP, conforme estejam em causa dados de base ou dados de tráfego, respetivamente.

¹⁰⁹ Neste sentido, RUI CARDOSO, “A conservação (...)”, cit., p. 72 e SÓNIA FIDALGO, “Conservação de Metadados – O Acórdão n.º 268/2022”, in *Revista Portuguesa de Direito Constitucional*, n.º 3, 2023, p. 56, disponível em: <https://rpdc.pt>. Contudo, este é um problema que já não se coloca com a aprovação da Lei n.º 18/2024, que procedeu à alteração da Lei n.º 32/2008.

¹¹⁰ No sentido de que a competência do art. 282.º, n.º 3 da CRP é de “exercício vinculado”, embora referindo que tem de haver uma decisão expressa para que haja reabertura do caso julgado, JORGE MIRANDA e RUI MEDEIROS – cfr. RUI MEDEIROS, “Artigo 282.º”, in *Constituição Portuguesa Anotada*, Tomo III, Coimbra, Coimbra Editora, 2007, pp. 837 e 838.

¹¹¹ Neste sentido, ANA TERESA CARNEIRO, “A inconstitucionalidade da “lei dos metadados” e o recurso extraordinário de revisão. Uma caixa de pandora?”, in *Liber Amicorum Benedita Mac Crorie*, vol. I, Braga, UMinho Editora, 2022, pp. 115 e 116, Ac. TC n.º 232/2004, Proc. n.º 807/99, disponível em: <http://www.tribunalconstitucional.pt> e Acs. STJ de 07/12/2023, Proc. n.º 2766/11.3TABRR-F.S1 e de 19/12/2023, Proc. n.º 191/17.1JELSB-K.S1, disponíveis em: <http://www.dgsi.pt>.

¹¹² Veja-se os Projetos de Lei n.º 70/XV/1ª (PSD), n.º 79/XV/1ª (CHEGA) e n.º 100/XV/1ª (PCP), disponíveis em: <https://www.parlamento.pt>.

¹¹³ Proposta de Lei n.º 11/XV/1ª, disponível em: <https://www.parlamento.pt>.

Contudo, dando conta da insuficiência destes dados para efeitos de investigação criminal, o Governo concluiu pelo aditamento de certos dados a esta mesma disposição, como a IMSI, a IMEI e o endereço de protocolo IP.

Com o objetivo de harmonizar as várias iniciativas legislativas, criou-se, na AR, um grupo de trabalho, do qual resultou o Decreto da AR n.º 91/XV, aprovado em votação final global¹¹⁴.

Este, procedendo à alteração da Lei n.º 32/2008, previu, em particular: a conservação dos dados no território da UE; a redução do prazo de conservação dos dados de tráfego e de localização¹¹⁵; um reforço das condições de segurança dos dados conservados; a competência exclusiva do MP para requerer a autorização de transmissão dos dados e a notificação do despacho da referida autorização ao titular dos mesmos¹¹⁶.

Não obstante, nada se alterou quanto à conservação generalizada e indiscriminada dos dados de tráfego e de localização¹¹⁷.

Por esta razão, e questionando-se ainda se a notificação ao titular dos dados satisfazia as exigências do Ac. do TC, o PR decidiu submeter o mesmo a fiscalização preventiva da constitucionalidade, o que resultou no Ac. n.º 800/2023¹¹⁸.

A decisão do TC não foi, para nós, inesperada, tendo este se pronunciado pela inconstitucionalidade da norma constante do art. 2.º do Decreto n.º 91/XV, na parte em que altera o art. 4.º da Lei n.º 32/2008, conjugado com o art. 6.º da mesma Lei, relativamente aos dados de tráfego e de localização, por esta violar os n.ºs 1 e 4 do art. 35.º e o n.º 1 do art. 26.º, em conjugação com o n.º 2 do art. 18.º, todos da CRP¹¹⁹.

Com efeito, não tendo o âmbito subjetivo da medida de conservação dos dados referidos sido alterado¹²⁰, a norma do Decreto n.º 91/XV, no que a isto diz respeito, não

¹¹⁴ Aprovação a 13/10/2023, com votos a favor do PS, PSD e CHEGA e votos contra da IL, PCP, BE e Livre, disponível em: <https://www.parlamento.pt>.

¹¹⁵ É estabelecido um prazo de três meses a contar da data da conclusão da comunicação, prorrogado até seis meses, salvo oposição do titular dos dados. De qualquer forma, a prorrogação dos prazos de conservação pode ir até ao limite de um ano, mediante autorização judicial, requerida pelo Procurador-Geral da República.

¹¹⁶ Art. 2.º do Decreto da AR n.º 91/XV, na parte em que altera os arts. 4.º, 6.º e 9.º da Lei n.º 32/2008.

¹¹⁷ Como interpretamos, o legislador português recusou a adoção de um sistema de conservação seletiva, atendendo à sua impraticabilidade e menor eficácia relativamente à conservação generalizada e indiferenciada. A mesma decisão foi tomada pelos legisladores estónio e sueco, considerando-o ineficaz. – cfr. Relatório de informação n.º 110 (2023-2024), Comissão do Senado Francês, 15/11/2023, disponível em: <https://www.senat.fr/rap/r23-110/r23-110.html>. Neste sentido, declaração de voto de JOANA FERNANDES COSTA ao Ac. TC n.º 800/2023, Proc. n.º 1130/2023, disponível em: <http://www.tribunalconstitucional.pt>.

¹¹⁸ Ac. TC n.º 800/2023, Proc. n.º 1130/2023, disponível em: <http://www.tribunalconstitucional.pt>.

¹¹⁹ *Ibidem*, 37 a 39.

¹²⁰ Não obstante o prazo de conservação ter sido reduzido.

se conforma com o entendimento preconizado no Ac. n.º 268/2022, razão pela qual se manteve o juízo de inconstitucionalidade¹²¹.

Quanto às restantes normas cuja apreciação foi requerida – as normas do art. 2.º do Decreto n.º 91/XV que alteram os arts. 4.º¹²² e 9.º¹²³ da Lei n.º 32/2008 – o TC decidiu não se pronunciar pela sua inconstitucionalidade.

Capítulo IV – Análise Crítica

1. Os direitos fundamentais em discussão

À primeira vista, poder-se-á dizer que temos, de um lado, o direito à segurança (art. 27.º da CRP) e, de outro lado, os direitos ao livre desenvolvimento da personalidade e à reserva sobre a intimidade da vida privada (art. 26.º, n.º 1 da CRP) e o direito à autodeterminação informativa (art. 35.º, n.ºs 1 e 4 da CRP), de que os detentores dos dados são titulares.

No caso de dados de tráfego que pressuponham uma comunicação entre pessoas, surge, ainda, o direito à inviolabilidade das comunicações (art. 34.º, n.ºs 1 e 4 da CRP), que abrange tanto o conteúdo em transmissão, como o tráfego enquanto tal (espécie, hora, duração, ...) ¹²⁴.

Ultrapassada a conceção liberal do Estado, todos estes direitos fundamentais apresentam, hoje, uma dimensão negativa, que exige a não interferência dos poderes públicos, e uma dimensão positiva, impondo aos mesmos um dever de proteção.

Se é inquestionável que a noção de liberdade se revela intrínseca a todos estes direitos, é igualmente certo que esta só é plenamente realizada se a segurança for garantida¹²⁵, verificando-se, assim, uma relação de reciprocidade e interdependência entre ambas.

¹²¹ Não se percebe, contudo, a razão pela qual, no ponto 39, o TC considera que tanto o teste da necessidade, como o da proporcionalidade em sentido estrito não foram superados pelo legislador, quando, no nosso entender, no Ac. n.º 268/2022, apenas se considerou como não preenchido este último subprincípio.

¹²² Previsão da necessidade de os dados serem conservados no território da UE.

¹²³ Previsão da competência exclusiva do MP para requerer a autorização de transmissão dos dados e a notificação do despacho da referida autorização ao titular dos mesmos.

¹²⁴ BENJAMIM SILVA RODRIGUES, *Da Prova (...)*, cit., p. 389, RITA CASTANHEIRA NEVES, *As ingerências (...)*, p. 31, e Acs. TC n.º 403/2015, Proc. n.º 773/15, 15, n.º 268/2022, Proc. n.º 828/2019, 10, disponíveis em: <http://www.tribunalconstitucional.pt>. Contra, MARIANA GOMES MACHADO, *O acesso aos metadados pelos serviços de informações da República Portuguesa*, Coimbra, Almedina, 2019, p. 129.

¹²⁵ Exigindo que as autoridades de investigação criminal sejam dotadas de meios capazes para prevenir e sancionar o cometimento de crimes graves.

A segurança¹²⁶, além de ser um direito fundamental, é também um dever do Estado, constituindo, a este nível, um valor constitucional da comunidade, passível de justificar a restrição de direitos fundamentais, nos termos do n.º 2 do art. 18.º da CRP¹²⁷.

Sob outro ângulo, o direito ao desenvolvimento da personalidade pretende tutelar a individualidade, isto é, a capacidade de a pessoa desenvolver as suas características, o seu modo de pensar e de agir¹²⁸. Este direito abrange, nomeadamente, o direito à autodeterminação comunicativa e o direito à confidencialidade dos dados pessoais¹²⁹.

O direito à reserva sobre a intimidade da vida privada apresenta-se como uma das dimensões do direito ao desenvolvimento da personalidade, tutelando os indivíduos contra o acesso a informações relativas à vida privada¹³⁰. Neste contexto, surge o direito à autodeterminação informativa, um verdadeiro direito fundamental que visa impedir que o indivíduo seja visto como um “simples objeto de informações”¹³¹.

Contudo, estes não são os únicos direitos fundamentais que relevam.

Não podemos esquecer, aqui, a condição especialmente frágil das vítimas de crimes graves, titulares de importantes direitos fundamentais, como o direito à vida, à segurança, à liberdade e à integridade física e psicológica.

Além disto, podendo as provas resultantes dos metadados contribuir tanto para confirmar a prática de crimes pelo arguido, como para demonstrar a sua inocência, não se constata, aqui, uma proteção exclusiva das vítimas. Os direitos dos próprios arguidos são, igualmente, garantidos, podendo a sua defesa revelar-se particularmente difícil na impossibilidade de utilização de tais provas¹³².

¹²⁶ Sobre este direito, veja-se JORGE BACELAR GOUVEIA, *Direito da Segurança: Cidadania, soberania e cosmopolitismo*, Coimbra, Almedina, 2018.

¹²⁷ Os direitos fundamentais não são, assim, absolutos – veja-se os arts. 26.º, n.º 4, 34.º, n.º 4 e 35.º, n.ºs 3 e 4, todos da CRP.

¹²⁸ FELIPE ARADY MIRANDA, “O direito fundamental ao livre desenvolvimento da personalidade”, in *Revista do Instituto do Direito Brasileiro*, ano 2, n.º 10, FDUL, Lisboa, p. 11177.

¹²⁹ A respeito destes direitos, veja-se o Ac. TC n.º 268/2022, Proc. n.º 828/2019, 11, disponível em: <http://www.tribunalconstitucional.pt>.

¹³⁰ MARIANA GOMES MACHADO, *O acesso (...)*, cit., p. 24.

¹³¹ GOMES CANOTILHO, VITAL MOREIRA, *Constituição da República Portuguesa Anotada*, Coimbra, Coimbra Editora, 3.ª ed., 1993, p. 216, *apud* CATARINA SARMENTO E CASTRO, *Direito da informática, privacidade e dados pessoais*, Coimbra, Almedina, 2005, p. 33.

¹³² Neste sentido, DUARTE RODRIGUES NUNES, “Impedirá (...)”, cit., p. 41 e declaração de voto de JOÃO CARLOS LOUREIRO ao Ac. TC n.º 800/2023, Proc. n.º 1130/2023, disponível em: <http://www.tribunalconstitucional.pt>.

2. A conservação dos dados de tráfego e de localização

Considerando a natureza pouco invasiva da privacidade dos dados de base, é ao nível dos dados de tráfego e de localização que se colocam as maiores dificuldades.

Com efeito, estes últimos, ao permitirem inferir informações sobre aspetos da vida privada de um indivíduo, atingem, de forma mais intensa, os seus direitos fundamentais¹³³.

Assim, sendo o regime de conservação de dados de base, tal como previsto na Lei n.º 32/2008¹³⁴, tido como conforme ao DUE e à Constituição, concentraremos a nossa análise no regime dos dados de tráfego e de localização.

Primeiramente, importa discorrer sobre a relação entre a ordem jurídica interna e o DUE.

Conservando o DUE autonomia face à ordem jurídica interna, a incompatibilidade entre normas nacionais e europeias simultaneamente aplicáveis a um determinado caso concreto é resolvida ao nível da eficácia: cabe ao juiz nacional desaplicar as normas nacionais sempre que estas contradigam as normas europeias.

Esta situação decorre do princípio do primado do DUE, implicitamente reconhecido na parte inicial do art. 8.º, n.º 4 da CRP, que estabelece a “prevalência tendencial do DUE sobre as normas de direito interno, inclusivamente sobre as normas de direito constitucional”¹³⁵⁻¹³⁶.

Não obstante, acompanhando o entendimento do TC, o art. 8.º, n.º 4 da CRP implica um segundo momento de interpretação, imposto pela sua parte final de “sentido contralimitador” (“com respeito pelos princípios fundamentais do Estado de direito democrático”), respeitando esta à relação entre o DUE e a CRP¹³⁷.

¹³³ Em particular os direitos à reserva sobre a intimidade da vida privada e à autodeterminação informativa.

¹³⁴ Prevê-se a conservação generalizada e indiferenciada pelo período de um ano a contar da data de conclusão da comunicação. Nos termos da Lei n.º 18/2024, este regime aplica-se, ainda, aos endereços de protocolo IP atribuídos à fonte de uma ligação, respeitando, assim, o entendimento do TJUE (art. 6.º, n.º 1, al. c) da Lei n.º 32/2008).

¹³⁵ RUI MEDEIROS, *A Constituição Portuguesa Num Contexto Global*, Lisboa, 2015, p. 378, cit. no Ac. TC n.º 422/2020, Proc. n.º 528/2017, 2.6.2.2, disponível em: <http://www.tribunalconstitucional.pt>.

¹³⁶ Quanto à relação entre o DUE e a ordem constitucional, são várias as interpretações feitas do art. 8.º, n.º 4 da CRP: uns adotam uma posição de aceitação sem limites do primado do DUE (FREITAS DO AMARAL, FAUSTO DE QUADROS), outros defendem o primado da Constituição (MIGUEL GALVÃO TELES, BLANCO DE MORAIS), havendo ainda quem considere um primado aplicativo do DUE (GOMES CANOTILHO, VITAL MOREIRA). – cfr. JORGE MIRANDA, “Artigo 8.º”, in *Constituição da República Portuguesa*, Tomo I, 2.ª ed. revista, Lisboa, UCP Editora, 2017, p. 129.

¹³⁷ Ac. TC n.º 422/2020, Proc. n.º 528/2017, 2.6.2.2, disponível em: <http://www.tribunalconstitucional.pt>.

Neste sentido, apesar da generosidade do texto constitucional presente na 1.^a parte do artigo, no que se refere ao respeito pelos limites constitucionais à aplicabilidade do DUE na nossa ordem interna, a última palavra não pode deixar de estar reservada ao TC¹³⁸.

O TC assume, assim, aquilo que se designa na teoria da jurisdição como “competência da competência”¹³⁹, cabendo ao mesmo decidir definitivamente todas as questões a respeito da sua própria competência, a qual é por si igualmente determinada.

Apesar disto, a ativação deste contralimite pressupõe a incompatibilidade com um princípio fundamental do Estado de direito democrático que, no âmbito da ordem europeia, não goze de um “valor materialmente paramétrico equivalente” ao que lhe é reconhecido na CRP.

Ora, esta situação é rara, sobretudo se atentarmos nos direitos fundamentais, cujo conteúdo e garantia já se encontram cobertos pelo DUE, gozando de um nível de proteção funcionalmente equivalente ao proporcionado pela jurisdição nacional¹⁴⁰.

Posto isto, e não obstante esta última consideração, ainda que haja “identidade material do princípio da proporcionalidade *enquanto tal* (artigo 52.º, n.º 1 da CDFUE e artigo 18.º, n.º 2 da CRP)”¹⁴¹, estamos convictos de que a forma como este é aplicado pelo TJUE, gera uma tensão inevitável com certos princípios estruturantes de um Estado de Direito, como os princípios da igualdade (art. 13.º da CRP), da presunção da inocência (art. 32.º, n.º 2 da CRP) e da proibição do défice (*Untermaßverbot*)¹⁴², não assegurando o “respeito, garantia e efetivação dos direitos e liberdades fundamentais” (art. 2.º da CRP).

¹³⁸ RUI MEDEIROS, *A Constituição Portuguesa Num Contexto Global*, Lisboa, 2015, p. 389, cit. no Ac. TC n.º 422/2020, Proc. n.º 528/2017, 2.6.2.2, disponível em: <http://www.tribunalconstitucional.pt>.

¹³⁹ Sobre este conceito, veja-se MIGUEL GALVÃO TELES, “A Competência da Competência do Tribunal Constitucional”, in *Legitimidade e Legitimação da Justiça Constitucional*, Coimbra, 1995, pp. 105-125.

¹⁴⁰ Ac. TC n.º 422/2020, Proc. n.º 528/2017, 2.6.2.2 e 2.7, disponível em: <http://www.tribunalconstitucional.pt>.

¹⁴¹ Declaração de voto de LINO RIBEIRO ao Ac. TC n.º 268/2022, Proc. n.º 828/2019, disponível em: <http://www.tribunalconstitucional.pt>. Com efeito, tanto na ordem interna, como na ordem europeia, o princípio da proporcionalidade desdobra-se em três exigências: a adequação das medidas aos fins; a necessidade ou exigibilidade das medidas e a proporcionalidade em sentido estrito. Contra esta subdivisão tradicional em três subprincípios, por considerar que não resolve os casos difíceis, JORGE REIS NOVAIS, *Princípios Estruturantes de Estado de Direito*, Coimbra, Almedina, 2021, p. 107.

¹⁴² Embora geralmente tido como uma vertente do princípio da proporcionalidade, atribuímos-lhe uma autonomia dogmática, uma vez que a estrutura tripolar própria do princípio da proporcionalidade carece de sentido no controlo de insuficiência. – Neste sentido, JORGE REIS NOVAIS, *Princípios (...)*, cit., p. 181.

Por isto, entendemos que o TC, detentor da última palavra nas questões da sua competência, não pode simplesmente fechar os olhos a esta realidade, conformando-se com a posição do TJUE, por força do princípio do primado do DUE.

Vejamos, então, de que forma este entendimento se impõe.

No que respeita ao subprincípio da adequação, nada temos a acrescentar à posição do TJUE e do TC. Sendo os metadados um instrumento útil às investigações penais, a sua conservação é adequada às finalidades de prevenção, deteção e repressão de crimes graves¹⁴³, sendo idónea à proteção de valores constitucionalmente protegidos, como a segurança interna e a legalidade democrática¹⁴⁴.

Os problemas surgem, porém, na análise dos subprincípios da necessidade e da proporcionalidade em sentido estrito.

Começando pelo crivo da necessidade ou exigibilidade, há que verificar se existe, relativamente ao meio escolhido, uma medida menos intrusiva que seja, em princípio, tão eficaz como aquela para atingir o mesmo fim¹⁴⁵.

Neste âmbito, não conseguimos acompanhar a metodologia do TJUE, nos termos da qual a conservação e o acesso, por constituírem ingerências distintas nos direitos fundamentais¹⁴⁶, são objeto de uma análise separada. Nestes termos, a “gravidade da ingerência que a conservação constitui é feita necessariamente em função do risco, para a vida privada das pessoas em causa”¹⁴⁷, não estando, por isso, dependente do regime de acesso adotado.

Ora, é precisamente este risco que nos leva a defender outra posição, uma vez que o mesmo só se materializa com o acesso aos dados.

Neste sentido, a mera conservação, não revelando quaisquer informações, é apenas suscetível de causar uma ingerência nos direitos fundamentais dos titulares dos dados¹⁴⁸. A inferência de informações detalhadas sobre a vida privada dos mesmos apenas se torna possível com o acesso¹⁴⁹.

¹⁴³ Ac. *Digital Rights Ireland*, §49.

¹⁴⁴ Ac. TC n.º 268/2022, Proc. n.º 828/2019, 17.2, disponível em: <http://www.tribunalconstitucional.pt>.

¹⁴⁵ Não se exige, contudo, que tenha o *mesmo* nível de eficácia, sob pena de este subprincípio se ter como facilmente observado. – Neste sentido, declaração de voto de JOÃO CARLOS LOUREIRO ao Ac. TC n.º 800/2023, Proc. n.º 1130/2023, disponível em: <http://www.tribunalconstitucional.pt>.

¹⁴⁶ Ac. *SpaceNet*, §91.

¹⁴⁷ *Ibidem*, §89.

¹⁴⁸ Neste sentido, DUARTE RODRIGUES NUNES, “Impedirá (...)”, cit., p. 29.

¹⁴⁹ O que justifica, a nosso ver, a competência exclusiva do MP para requerer a autorização de transmissão dos dados e a intervenção do JIC, enquanto juiz das garantias (implicando estar-se na fase de inquérito).

Para tal entendimento concorre o estipulado no art. 7.º, n.º 2 da Lei n.º 32/2008, nos termos do qual os dados devem permanecer bloqueados desde o início da sua conservação, só sendo desbloqueados em caso de transmissão às autoridades competentes¹⁵⁰.

Além disto, os dados são conservados para, se necessário, serem transmitidos às autoridades competentes (arts. 1.º, 3.º, n.º 1 e 7.º, n.º 1, al. a) da Lei n.º 32/2008)¹⁵¹, pelo que uma análise separada destes dois momentos não se revela adequada.

Destarte, a este respeito, concordamos com a orientação do TC, propugnando uma compreensão conjugada da conservação e acesso aos metadados. De facto, julgamos que “um maior rigor do legislador no acesso e na transmissão dos dados conservados pode (...) autorizar uma maior amplitude no domínio da sua conservação”¹⁵²⁻¹⁵³.

Por assim ser, importa atender às garantias efetivas contra o risco de acessos ilícitos e abusivos aos dados conservados que constam na Lei n.º 32/2008¹⁵⁴.

Entre estas, destacam-se: as condições de segurança do art. 7.º referidas *supra*¹⁵⁵; o controlo destas por parte de uma entidade administrativa independente (CNPD – art. 7.º, n.º 7); a competência exclusiva do MP para requerer a autorização de transmissão dos dados (agora prevista no art. 9.º, n.º 2); a autorização de transmissão dos dados pelo JIC (art. 9.º, n.º 1); o acesso aos dados exclusivamente por pessoas especialmente autorizadas (arts. 7.º, n.º 1, al. d) e 8.º); a notificação do despacho de autorização de acesso ao titular dos dados (agora prevista no art. 9.º, n.ºs 7 e 8) e a constituição de crime em caso de incumprimento das regras de segurança do art. 7.º, não bloqueio dos dados ou acesso aos mesmos por pessoa não especialmente autorizada (art. 13.º).

¹⁵⁰ Esta deve observar o mais elevado grau de codificação e proteção possível (art. 7.º, n.º 3 da Lei n.º 32/2008), sendo os dados destruídos no final do prazo de conservação (arts. 7.º, n.º 1, al. e) e 11.º da Lei n.º 32/2008), o que garante a confidencialidade dos dados pessoais (art. 5.º, n.º 1, al. f) do RGPD, art. 5.º da Diretiva 2002/58/CE e arts 26.º e 35.º da CRP).

¹⁵¹ Permitido pelo art. 35.º, n.ºs 1 e 4 da CRP.

¹⁵² Ac. TC n.º 268/2022, Proc. n.º 828/2019, 14, disponível em: <http://www.tribunalconstitucional.pt>. Neste ponto, o TC refere que a alteração da sua metodologia se imporia caso a mesma resultasse num juízo de não inconstitucionalidade, incompatível com os parâmetros da CDFUE. Ora, para além de entendermos que a sua orientação impunha, na verdade, um juízo de não inconstitucionalidade, devido às regras de segurança e acesso estritas presentes na Lei n.º 32/2008, não concordamos com esta justificação, uma vez que quem tem a “competência da competência” é o TC.

¹⁵³ Neste sentido, declaração de voto de LINO RIBEIRO ao Ac. TC n.º 268/2022, Proc. n.º 828/2019 e declarações de voto de JOANA FERNANDES COSTA e MARIA BENEDITA URBANO ao Ac. TC n.º 800/2023, Proc. n.º 1130/2023, disponíveis em: <http://www.tribunalconstitucional.pt> e DUARTE RODRIGUES NUNES, “Impedirá (...)”, cit., pp. 28 e 29.

¹⁵⁴ É de salientar, aqui, a diferença entre acesso ilícito e acesso abusivo: enquanto o primeiro corresponde a um acesso contrário à lei, por parte de indivíduos sem direito de acesso (por ex., *hackers*), o segundo verifica-se quando titulares de um direito de acesso (por ex., autoridades de investigação criminal) o exercem de forma abusiva.

¹⁵⁵ E reforçadas pelas alterações introduzidas pela Lei n.º 18/2024 (art. 7.º, n.ºs 4, 5 e 6 da Lei n.º 32/2008).

Uma outra garantia importante diz respeito à existência de prazos de conservação curtos¹⁵⁶.

Contrariamente ao Decreto da AR n.º 91/XV, nos termos da atual Lei n.º 32/2008, a conservação dos dados de tráfego e de localização, embora sujeita a outra condição a que faremos referência *infra*, encontra-se submetida a um prazo limitado ao “estritamente necessário” (art. 6.º, n.º 5). Isto significa que, estando dependente do caso concreto, o prazo de armazenamento pode não ser necessariamente um prazo curto.

Apesar de reconhecermos a impossibilidade de determinarmos o prazo de conservação adequado¹⁵⁷, consideramos que o princípio da legalidade¹⁵⁸ impõe uma determinabilidade que a atual Lei n.º 32/2008 não oferece, apresentando-se a solução do Decreto da AR n.º 91/XV mais clara e precisa.

Posto isto, acreditamos que todas estas garantias conferem legitimidade à conservação generalizada e indiferenciada de dados de tráfego e de localização, tendo em conta que o seu potencial lesivo é por elas fortemente restringido.

Não adotando esta lógica, o TJUE entende que a mera conservação indiscriminada dos referidos dados excede os limites do estritamente necessário¹⁵⁹, propondo outras medidas, nomeadamente, a conservação rápida e a conservação seletiva¹⁶⁰.

Data venia, a argumentação do TJUE revela-se insuficiente neste ponto. O Tribunal limita-se a apresentar outras soluções, nunca demonstrando que as mesmas são equivalentemente eficazes na realização do mesmo fim, quando comparadas com a conservação generalizada e indiferenciada.

Acreditando que esta apresenta uma eficácia particular no combate à criminalidade grave, procuraremos explicar como nenhuma das alternativas pode ser tida como equivalente à mesma.

¹⁵⁶ Não compreendemos como, no Ac. *SpaceNet*, o TJUE entendeu que, apesar dos prazos de conservação curtos previstos na legislação alemã, a conservação dos dados de tráfego e de localização “apresenta, de qualquer modo, um caráter grave independentemente da duração do período de conservação (...)” – cfr. Ac. *SpaceNet*, §88. Se a conservação de dados de tráfego e de localização, devido à sua natureza especialmente invasiva da privacidade, se pode revelar particularmente grave, essa gravidade é tanto menor quanto mais curto for o prazo de armazenamento. – Neste sentido, declarações de voto de JOANA FERNANDES COSTA e MARIA BENEDITA URBANO ao Ac. TC n.º 800/2023, Proc. n.º 1130/2023, disponíveis em: <http://www.tribunalconstitucional.pt>.

¹⁵⁷ Uma vez que tal exige a participação das várias entidades-chave.

¹⁵⁸ Na sua vertente de lei certa (art. 29.º, n.ºs 1 e 3 da CRP).

¹⁵⁹ Ac. *Tele 2*, §107, Ac. *La Quadrature du Net*, §141, Ac. *Commissioner of An Garda Síochána*, §65 e Ac. *SpaceNet*, §88.

¹⁶⁰ Esta situação leva-nos a questionar se o TJUE não estará a assumir o papel do legislador. – cfr. IAIN CAMERON, “*A. Court (...)*”, cit., p. 1489.

A conservação rápida (*quick freeze*), sendo relativa a uma pessoa específica e direcionada, geralmente não se revela útil no âmbito da investigação de crimes graves, uma vez que dificilmente se consegue identificar, de forma antecipada, os dados essenciais à descoberta da verdade¹⁶¹.

Ademais, sendo este pedido feito, designadamente, aos fornecedores de serviços, o mesmo fica dependente dos dados conservados por estes para fins comerciais¹⁶², os quais são insuficientes para efeitos de investigação criminal.

Exemplificando, os dados de localização, além de raramente serem úteis para efeitos de faturação¹⁶³, só podem ser objeto de tratamento se forem tornados anónimos (art. 7.º, n.º 1 da Lei n.º 41/2004), não relevando, assim, para a investigação.

É, também, frequente os fornecedores de serviços, dos dados que têm permissão para conservar, armazenarem apenas uma parte deles¹⁶⁴.

Por esta razão, optar-se exclusivamente pelo acesso por parte das autoridades competentes aos dados conservados pelas operadoras de comunicações para fins comerciais seria, igualmente, inútil¹⁶⁵.

De resto, a insuficiência destes dados foi já concluída pelo TJUE, quando defendeu a admissibilidade da conservação de endereços IP, e pelo Governo, na sua Proposta de Lei n.º 11/XV/1ª, quando acrescenta outros dados além dos necessários para efeitos de faturação¹⁶⁶.

Não se garante, assim, a disponibilidade de dados históricos, permitida pela conservação generalizada e indiscriminada e, em muitos casos, indispensável para a identificação de suspeitos¹⁶⁷.

¹⁶¹ Conclusões do Advogado-Geral Henrik Saugmandsgaard Øe, 19 de julho de 2016, §213, disponível em: <https://eur-lex.europa.eu/homepage.html>.

¹⁶² Veja-se *European Commission, Directorate-General For Migration And Home Affairs*, CLAIRE DUPONT, VALENTINA CILLI, et al., *Study on the retention of electronic communications non-content data for law enforcement purposes – Final report*, Publications Office, 2020, pp. 96, 97 e 121, disponível em: <https://data.europa.eu/doi/10.2837/384802>.

¹⁶³ Pense-se no caso de *roaming*.

¹⁶⁴ Por ex., no caso de pacotes ilimitados, os dados relativos às chamadas efetuadas, não sendo úteis para efeitos de faturação, não são conservados. – cfr. Declaração de voto de JOANA FERNANDES COSTA ao Ac. TC n.º 800/2023, Proc. n.º 1130/2023, disponível em: <http://www.tribunalconstitucional.pt>.

¹⁶⁵ Neste âmbito, não compreendemos como a existência de uma base de dados autónoma para fins de investigação criminal pode comportar um maior risco de abuso, pois trata-se de um armazenamento de dados no mesmo fornecedor de serviços, sem que as condições de segurança fiquem comprometidas. – cfr. Declaração de voto de JOÃO CARLOS LOUREIRO o Ac. TC n.º 800/2023, Proc. n.º 1130/2023, disponível em: <http://www.tribunalconstitucional.pt>.

¹⁶⁶ Quanto a este aspeto, veja-se a crítica da CNPD no Parecer n.º 2022/50, disponível em: <https://www.cnpd.pt>.

¹⁶⁷ Veja-se Comissão Europeia, *Relatório de Avaliação sobre a Directiva relativa à conservação de dados (2006/24/CE)*, Bruxelas, 2011, p. 6, disponível em: <https://eur-lex.europa.eu/homepage.html> e *European Commission, Commission Staff Working Document – Annex to the Proposal for a Directive of the European*

Relativamente à conservação seletiva, na análise da sua eficácia, iremos tomar como exemplo os países que já adotaram esta solução, como a Bélgica e a Dinamarca.

A Bélgica apresenta, desde 2022, um sistema misto, que combina a conservação generalizada, prevista para certo tipo de infrações penais, e a conservação seletiva, para efeitos de prevenção de ameaças graves à segurança pública e da criminalidade grave. Esta última assenta em dois critérios geográficos: os dados são automaticamente conservados em zonas particularmente expostas a ameaças de criminalidade grave ou de violação da segurança nacional (aeroportos, prisões, ...) e em zonas sujeitas a uma elevada taxa de criminalidade grave, consistindo esta no registo, em média, por ano e por 1000 habitantes, de pelo menos três infrações referidas nos §§2 a 4 do art. 90ter do *Code d'instruction criminelle*, nos três anos anteriores ao ano em curso¹⁶⁸.

A Dinamarca combina, igualmente, desde 2022, a conservação generalizada, prevista para efeitos da salvaguarda nacional, e a conservação seletiva, com vista à luta contra a criminalidade grave. Contudo, esta baseia-se tanto em categorias de pessoas, como em critérios geográficos, sendo, a conservação de dados automática: i) para as pessoas condenadas por infrações penais graves por um período de três a dez anos, bem como para os números de telemóvel sujeitos a uma ordem de interceção de comunicações, ii) em áreas cujo n.º de infrações penais graves comunicadas ou n.º de residentes condenados por estas for superior a 1,5 vezes a média nacional nos últimos três anos, estando ainda compreendidas “zonas sensíveis em termos de segurança” (aeroportos, embaixadas, ...)¹⁶⁹.

Várias são as críticas apontadas a estes regimes.

Quanto ao sistema belga, tem-se assinalado que a conservação de dados está dependente da existência de um certo n.º de infrações graves numa dada região.

Além disto, o limite mínimo de infrações revela-se problemático, nos seguintes termos: se for fixado demasiado baixo, a conservação direcionada pode converter-se numa conservação generalizada e indiferenciada; se for fixado demasiado alto, perde-se a finalidade da conservação de dados¹⁷⁰.

Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC, “Data Preservation versus Data Retention”, 2005, disponível em: <https://eur-lex.europa.eu/homepage.html>.

¹⁶⁸ Cfr. Relatório de informação n.º 110 (...), cit..

¹⁶⁹ Cfr. Relatório de informação n.º 110 (...), cit..

¹⁷⁰ Relatório Sueco, *Dataagring och åtkomst till elektronisk information*, Estocolmo, 2023, p. 253, disponível em: <https://www.regeringen.se>.

Sendo a média nacional da taxa de criminalidade na Bélgica de 11 infrações graves por 1000 habitantes durante três anos, o limite mínimo proposto pelo Governo acaba por permitir a cobertura alargada do território belga (ou até a sua totalidade)¹⁷¹.

Já o regime dinamarquês não atende à dimensão populacional das diferentes localidades, pelo que qualquer cidade acima de um determinado limiar, relativamente baixo para a sua dimensão populacional, é abrangida por estes critérios¹⁷².

Além disto, se a criminalidade aumentar de forma significativa e uniforme por todo o país, não se constata um aumento na conservação de dados¹⁷³.

Conforme a Polícia Nacional Dinamarquesa estimou, 11% da área geográfica da Dinamarca e 67% da população (3,9 milhões de pessoas) seriam abrangidas por esta medida.

Isto posto, estes exemplos demonstram que a conservação seletiva, pelo menos de acordo com os critérios propostos pelo TJUE, acaba por apresentar um alcance considerável, não se distanciando, assim, da conservação generalizada e indiferenciada.

Considerando estes modelos, entendemos, ainda, que a conservação seletiva não viabiliza o acesso aos dados, seja quem for a pessoa sobre quem recaia a suspeita da prática do crime¹⁷⁴, pondo em causa certos princípios fundamentais da Constituição.

Atendendo ao critério de categorias de pessoas, este não permite o acesso aos dados de uma pessoa que não esteja previamente identificada como suscetível de cometer tal infração.

Neste âmbito, no caso da conservação se dirigir contra pessoas “que sejam objeto de inscrição no registo criminal nacional que mencione uma condenação anterior por atos de criminalidade grave que possam implicar um risco elevado de reincidência”¹⁷⁵, está-se, na realidade, a suspeitar que as mesmas possam voltar a cometer crimes, sem que

¹⁷¹ PATRICK BREYER, *Conservation “ciblée” des données : cartographier ce que le gouvernement belge veut cacher*, de 08/06/2022, disponível em: <https://www.patrick-breyer.de/en/conservation-ciblee-des-donnees-cartographier-ce-que-le-gouvernement-belge-veut-cacher/>. O legislador belga, inclusivamente, descreveu o novo regime como “direcionado na sua abordagem, mas generalizado nas suas consequências”. – cfr. *Chambre des représentants, Projet de Loi relatif à la collecte et à la conservation des données d’identification et des métadonnées dans le secteur des communications électroniques et à la fourniture de ces données aux autorités*, de 17/03/2022, disponível em: <https://www.lachambre.be/FLWB/PDF/55/2572/55K2572001.pdf>.

¹⁷² JESPER LUND, *The new Danish data retention law: attempts to make it legal failed after just six days*, de 15/06/2022, disponível em: <https://itpol.dk/articles/new-Danish-data-retention-law-2022>.

¹⁷³ Relatório Sucoo, *Datalagring* (...), cit., p. 254.

¹⁷⁴ Declaração de voto de JOANA FERNANDES COSTA ao Ac. TC n.º 800/2023, Proc. n.º 1130/2023, disponíveis em: <http://www.tribunalconstitucional.pt>.

¹⁷⁵ Ac. *SpaceNet*, §107.

exista notícia dos mesmos, não se respeitando, assim, o princípio da presunção da inocência (art. 32.º, n.º 2 da CRP).

Além disso, resultando esta diferença de tratamento da especial vulnerabilidade deste grupo de pessoas a preconceitos e projetando-se a mesma na diminuição do seu *status* na comunidade política¹⁷⁶, o princípio de igualdade (art. 13.º da CRP) é, igualmente, violado. Aqui, importa atender ao art. 35.º, n.º 3 da CRP, segundo o qual o tratamento de dados relativos à vida privada é apenas possível com “garantias de não discriminação”¹⁷⁷.

Relativamente ao critério geográfico, o esclarecimento de crimes fica, inaceitavelmente, dependente do local onde o ilícito é cometido ou planeado, impedindo a investigação noutras partes do território se tais ilícitos forem aí cometidos¹⁷⁸.

Este tipo de critério favorece, assim, a criação de perfis discriminatórios de certas áreas¹⁷⁹, havendo o risco de deslocação das atividades ilícitas para uma zona não abrangida pela conservação de dados¹⁸⁰.

Levanta-se, ainda, a preocupação de vigilância permanente de “locais estratégicos”, como aeroportos, embaixadas ou zonas de portagens¹⁸¹.

Por tudo isto, julgamos que a dimensão formal do princípio de igualdade (art. 13.º, n.º 1 da CRP), de aplicação da lei sem olhar a quem, é aquela que conduz à solução mais justa¹⁸².

E não se alegue que este entendimento faz de todos nós suspeitos do cometimento de crimes graves. Antes pelo contrário. Por se presumir que todos somos inocentes, e na

¹⁷⁶ JORGE REIS NOVAIS, *Princípios (...)*, cit. p. 89.

¹⁷⁷ No sentido de que o entendimento do TJUE é incompatível com o art. 35.º, n.º 3 da CRP, veja-se declaração de voto de LINO RIBEIRO no Ac. TC n.º 268/2022, Proc. n.º 828/2019, disponível em: <http://www.tribunalconstitucional.pt>, DUARTE RODRIGUES NUNES, “Impedirá (...)”, cit., p. 40 e SÓNIA FIDALGO, “Conservação (...)”, cit., p. 58.

¹⁷⁸ Decisão do *Conseil d'État*, n.º 393099, de 21/04/2021, §54, disponível em: <https://www.conseil-etat.fr>. Isto cria diferentes oportunidades de combater o crime dentro de um país. – cfr. Relatório Sueco, *Datalagring (...)*, cit., p. 251.

¹⁷⁹ Neste sentido, CHLOÉ BERTHÉLÉMY, *Europe's data retention saga and its risks for digital rights*, de 02/09/2021, disponível em: <https://edri.org/our-work/europes-data-retention-saga-and-its-risks-for-digital-rights/>, BARBARA GRABOWSKA-MOROZ, “Data Retention in the European Union”, in *European Constitutional courts towards data retention*, vol. 45, Suíça, Springer Nature Switzerland AG, 2020, p. 13 e ORLA LYSKEY, *Tele2 Sverige AB and Watson et al: Continuity and Radical Change*, de 12/01/2017, disponível em: <https://europeanlawblog.eu/2017/01/12/tele2-sverige-ab-and-watson-et-al-continuity-and-radical-change/>.

¹⁸⁰ Conclusões do Advogado-Geral Henrik Saugmandsgaard Øe, cit., §214. Embora reconheçamos que as pessoas não saberão efetivamente quais as zonas abrangidas pela medida de conservação de dados.

¹⁸¹ IAIN CAMERON, “*A. Court (...)*”, cit., p. 1489.

¹⁸² Neste sentido, declaração de voto de MARIA BENEDITA URBANO ao Ac. TC n.º 800/2023, Proc. n.º 1130/2023, disponível em: <http://www.tribunalconstitucional.pt>.

impossibilidade de determinar objetivamente quem é suscetível de cometer um crime¹⁸³, a vivência em comunidade impõe uma conservação dos metadados de todas as pessoas, sob pena de se adotar medidas discriminatórias se assim não se entender¹⁸⁴.

No que toca à proporcionalidade em sentido estrito, há que avaliar a relação entre o bem que se pretende proteger com a restrição e o bem restringido afetado. Comparam-se as vantagens e desvantagens da restrição, sem se exigir que o meio seja o mais proporcional, sob pena de se cair num juízo essencialmente político¹⁸⁵.

Conforme referido, o TC entendeu que a agressão aos direitos fundamentais resultante desta conservação não é “contrapesada pelos efeitos positivos no combate à criminalidade”¹⁸⁶, porém não vemos como tal possa ser verdade.

Primeiramente, sob a nossa perspetiva, a restritividade que caracteriza o catálogo de crimes previsto na al. g) do n.º 1 do art. 2.º da Lei n.º 32/2008 concorre para a defesa da proporcionalidade da conservação indiscriminada de dados de tráfego e de localização¹⁸⁷.

Em segundo lugar, sendo a intensidade da ingerência resultante da conservação generalizada e indiferenciada dos dados referidos avaliada em função do risco de os mesmos permitirem tirar conclusões sobre a vida privada dos indivíduos em causa, este, além de se tornar real com o acesso, acaba por revelar uma menor gravidade no âmbito da realidade digital atual.

Com efeito, muitas empresas privadas recolhem, hoje, de forma indiscriminada, inúmeros dados pessoais¹⁸⁸ e são várias as pessoas que divulgam aspetos privados nas redes sociais, havendo, assim, um “grande fluxo de dados pessoais (...) sujeitos a ‘apropriação’ indevida”¹⁸⁹.

Argumenta-se que esta recolha e exposição são consentidas, o que, aliás, também se verifica quanto à conservação de dados pelos fornecedores de serviços para efeitos

¹⁸³ Fora o caso de já ter sido constituída uma suspeita, que, como referido, muitas vezes, só é garantido pela conservação generalizada e indiferenciada dos dados.

¹⁸⁴ De notar a comparação feita com a base de dados da Autoridade Tributária e dos serviços de inteligência do Estado prevista na declaração de voto de MARIA BENEDITA URBANO ao Ac. TC n.º 800/2023, Proc. n.º 1130/2023, disponível em: <http://www.tribunalconstitucional.pt>.

¹⁸⁵ JORGE REIS NOVAIS, *Princípios (...)*, cit., pp. 117 e 120.

¹⁸⁶ Ac. TC n.º 268/2022, Proc. n.º 828/2019, 18, disponível em: <http://www.tribunalconstitucional.pt>.

¹⁸⁷ Embora esta lista de crimes possa revelar-se insuficiente, atendendo ao desenvolvimento tecnológico. De igual forma, atenda-se à previsão de um maior catálogo no âmbito das escutas telefónicas, um meio de prova que, ao possibilitar a revelação de dados de conteúdo, se apresenta mais ofensivo de direitos fundamentais do que a conservação e acesso a metadados.

¹⁸⁸ Criando perfis de consumidores, em função das suas preferências.

¹⁸⁹ Declaração de voto de MARIA BENEDITA URBANO ao Ac. TC n.º 800/2023, Proc. n.º 1130/2023, disponível em: <http://www.tribunalconstitucional.pt>.

comerciais (art. 6.º, n.º 4 da Lei n.º 41/2004)¹⁹⁰. Contudo, não podemos desconsiderar o facto de, nos contratos de adesão a serviços de comunicações eletrónicas, se prever a possibilidade de transmissão dos dados conservados às autoridades competentes para fins de investigação criminal¹⁹¹. Não estarão as pessoas a aceitar essa possibilidade quando assinam o contrato?¹⁹²

Neste seguimento, se, de um lado, temos uma mera possibilidade de ingerência nos direitos fundamentais resultante da conservação de metadados, do outro lado, temos uma certeza de que esta é útil e, muitas vezes, imprescindível para a investigação de crimes graves, pelo que entendemos que o benefício obtido com a restrição é superior ao sacrifício por esta imposto.

Assim, o TJUE, ao colocar o legislador nacional perante a alternativa representada pela conservação seletiva ou a ausência de uma qualquer obrigação de conservação¹⁹³⁻¹⁹⁴, deixa as vítimas desprotegidas, privando-as da possibilidade de conhecer o autor do crime.

Neste quadro, o princípio da proibição do défice requer a análise da (in)suficiência da proteção a um direito em função das exigências constitucionais¹⁹⁵.

Existindo, manifestamente, um imperativo de tutela neste âmbito, atendendo aos bens jurídicos que decorrem dos direitos fundamentais de que as vítimas são titulares, é nosso entendimento que, sem a previsão de uma conservação generalizada e indiferenciada de dados de tráfego e de localização, a tutela concedida pelo Estado se revela insuficiente.

Se atentarmos, por exemplo, nos crimes de sequestro, rapto ou tomada de reféns, impedindo-se o conhecimento dos movimentos e interações anteriores do autor do crime¹⁹⁶, a investigação dos mesmos torna-se impossível, deixando as vítimas numa situação intolerável, à luz das exigências de um Estado social de Direito.

¹⁹⁰ Consentimento exigido como “forma de gestão de auto-restrições de direitos fundamentais”. – cfr. DOMINGOS SOARES FARINHO, “Comentário ao Acórdão n.º 268/2022 do Tribunal Constitucional português: a aplicação do princípio da proporcionalidade no controlo de restrições aos direitos à reserva da intimidade da vida privada e à autodeterminação informativa”, in *e-Pública - Revista Eletrónica de Direito Público*, Lisboa, vol. 10, n.º 2, 2023, p. 223.

¹⁹¹ Veja-se os contratos de adesão da Vodafone e da NOS, disponíveis, respetivamente, em: <https://www.vodafone.pt/content/dam/digital-sites/downloads/formularios/particulares/portabilidade-movel.pdf> e https://www.nos.pt/content/dam/nos/assets/pdfs/Proposta_de_subscricao.pdf.

¹⁹² Embora, compreensivelmente, o consentimento nunca seja exigível neste âmbito.

¹⁹³ Solução adotada na Alemanha e nos Países Baixos. – Cfr. Relatório de informação n.º 110 (...), cit..

¹⁹⁴ Declaração de voto de JOANA FERNANDES COSTA ao Ac. TC n.º 800/2023, Proc. n.º 1130/2023, disponíveis em: <http://www.tribunalconstitucional.pt>.

¹⁹⁵ JORGE REIS NOVAIS, *Princípios* (...), cit., pp. 191 e 192.

¹⁹⁶ Assegurado pela conservação generalizada e indiferenciada dos dados.

Assim sendo, não compreendemos como a argumentação invocada pelo TJUE, em prol da admissibilidade da conservação generalizada e indiferenciada dos endereços IP atribuídos à fonte de uma ligação¹⁹⁷, não vale, de igual modo, no âmbito dos dados de tráfego e de localização.

De facto, além da possibilidade de a investigação dos crimes ser inviável na ausência de uma medida de conservação indiscriminada destes dados, a suposição de que os endereços IP podem ser vistos como menos sensíveis revela-se equivocada, atendendo às suas capacidades de rastreamento¹⁹⁸.

3. A adoção da Lei n.º 18/2024

A Lei n.º 18/2024 procedeu à alteração da Lei n.º 32/2008, de forma a conformar as suas disposições com os Acs. do TC n.ºs 268/2022 e 800/2023.

No que respeita aos dados de tráfego e de localização, o legislador estabelece, agora, uma distinção entre: i) os que são conservados pelos fornecedores de serviços para efeitos de faturação ou por força de disposição legal especial e ii) os que não são armazenados nesses termos, sendo o regime aplicável a cada uma destas categorias de dados distinto.

Quanto a estes últimos, a atual redação da Lei n.º 32/2008 estabelece o seguinte: a sua conservação depende de uma “autorização judicial fundada na sua necessidade para a finalidade prevista no n.º 1 do artigo 3.º”¹⁹⁹ (art. 6.º, n.º 2); o pedido de autorização judicial tem carácter urgente, devendo ser decidido no prazo máximo de 72 horas (art. 6.º, n.º 3) e “de forma a salvaguardar a utilidade” deste pedido, o MP comunica de imediato aos fornecedores de serviços a submissão do mesmo, não podendo os dados ser eliminados até à decisão final sobre a respetiva conservação (art. 6.º, n.º 4).

Estas disposições suscitam-nos várias dúvidas.

Do art. 6.º, n.º 4, concluímos que o pedido de autorização judicial é feito pelo MP, o que implica que já esteja instaurado um processo de investigação do crime, com vista à identificação do suspeito.

¹⁹⁷ Assente na impossibilidade de investigação de infrações cometidas em linha sem a previsão desta medida. – cfr. Ac. *Quadrature du Net*, §§152, 154 e 155 e Ac. *SpaceNet*, §§100 a 102.

¹⁹⁸ ALENA BIRRER, DANYA HE, NATASCHA JUST, “The state is watching you – A cross-national comparison of data retention in Europe”, in *Telecommunications Policy*, 47, Elsevier, Países Baixos, 2023, p. 10.

¹⁹⁹ Esta autorização compete a uma formação das secções criminais do STJ (art. 6.º, n.º 7 da Lei n.º 32/2008 e arts. 47.º, n.º 4 e 54.º, n.º 4 da LOSJ – Lei n.º 62/2013).

Neste quadro, não se compreende de que forma a comunicação imediata do pedido por parte do MP aos fornecedores de serviços assegura a utilidade do mesmo. Se estes não podem conservar dados de tráfego e de localização sem autorização judicial²⁰⁰, entendemos que este artigo apenas permite o armazenamento dos referidos dados desde o momento em que é comunicado o pedido. Sendo assim, os dados são apenas conservados para o futuro, não sendo possível a reconstituição do passado.

Não se estará, assim, a prever, de forma encapotada, uma medida de preservação de dados, já existente no art. 12.º da LC, com a agravante de ser necessária uma autorização judicial?

Neste sentido, a crítica que apontámos a respeito da eficácia limitada da preservação de dados vale, aqui, de igual forma, continuando a conservação generalizada e indiferenciada dos dados em causa a ser a solução mais adequada.

Tendo já mencionado a falta de exatidão quanto ao prazo de conservação dos dados de tráfego e de localização prevista na atual Lei n.º 32/2008, a mesma constata-se no seu art. 6.º, n.º 2. Como se justifica a necessidade da conservação dos dados para a finalidade de investigação, deteção e repressão de crimes graves que fundamenta a autorização judicial? Recorrer-se-á aos critérios de seleção propostos pelo TJUE, com todas as consequências que daí decorrem?

Julgamos, ainda, que o recurso à expressão “por força de disposição legal especial” no referido artigo não se revela o mais adequado, pois questionamos se o art. 4.º da Lei n.º 32/2008 não poderá, ele mesmo, ser considerado uma disposição legal especial, impondo a conservação dos dados aos fornecedores de serviços.

Posto isto, esta solução, além de poder contribuir para a sobrecarga dos tribunais, não se mostra suficientemente útil à investigação de crimes graves, uma vez que não garante a disponibilidade de dados históricos.

Destarte, acreditamos que a alteração do regime previsto no Decreto da AR n.º 91/XV, que previa uma conservação generalizada e indiferenciada dos dados de tráfego e de localização e prazos curtos de armazenamento²⁰¹, pela Lei n.º 18/2024 determina uma perda de garantias no combate à criminalidade grave, pelo que o primeiro não deveria ter sido declarado inconstitucional.

²⁰⁰ Fora aqueles conservados pelos fornecedores de serviços para efeitos de faturação ou por força de disposição legal especial.

²⁰¹ Apenas sujeitando a autorização judicial a prorrogação dos prazos de conservação (art. 2.º do Decreto da AR n.º 91/XV, na parte em que altera o art. 6.º da Lei n.º 32/2008).

Por último, se dúvidas havia de que os dados tinham de ser conservados no território da UE, tal imposição encontra-se, agora, prevista no art. 4.º da Lei n.º 32/2008.

De igual forma, os problemas relativos ao acesso a metadados foram solucionados, prevendo-se, como referido, a competência exclusiva do MP para requerer a autorização de transmissão de dados (art. 9.º, n.º 2 da Lei n.º 32/2008) e a notificação do despacho da referida autorização ao titular dos mesmos (art. 9.º, n.ºs 7 e 8 da Lei n.º 32/2008).

Estipulou-se, ainda, a proibição de acesso aos dados por parte dos fornecedores de serviços, salvo nos casos previstos na lei ou definidos contratualmente com o cliente (art. 6.º, n.º 6 da Lei n.º 32/2008)²⁰² e os termos em que a transmissão dos dados a autoridades de outros Estados pode ter lugar (art. 9.º, n.º 9 da Lei n.º 32/2008).

Conclusões

I. Os metadados são dados gerados antes e durante uma comunicação, que contêm informação sobre aspetos importantes para a investigação de crimes graves. Compreendem, assim, os dados de base, necessários ao acesso à rede, e os dados de tráfego, necessários ao estabelecimento de uma comunicação e que integram a maioria dos dados de localização.

II. Devido à sua natureza particularmente invasiva da privacidade dos cidadãos, é ao nível dos dados de tráfego e de localização que se suscitam os principais problemas, revelando-se particularmente difícil encontrar a solução de conservação mais adequada, que otimize tanto a segurança comunitária, como o direito à privacidade do cidadão.

III. Em Portugal, são três os diplomas legais em vigor que regulam o acesso aos dados conservados pelos fornecedores de serviços de comunicações: o CPP (*maxime*, o art. 189.º, n.º 2), a Lei n.º 32/2008 e a LC. Este regime disperso, que deveria ter sido integrado no CPP, cria uma grande incerteza jurídica, atendendo às diferentes interpretações que suscita. No entanto, a conjugação das diferentes leis é possível: a Lei n.º 32/2008 e a LC reduziram o âmbito de aplicação do art. 189.º do CPP, apresentando áreas de aplicação distintas.

²⁰² Disposição que, a nosso ver, não era necessária, pois o acesso aos dados ocorria nos termos estabelecidos no art. 9.º da Lei n.º 32/2008.

IV. A Lei n.º 32/2008, que transpôs a Diretiva 2006/24/CE, impunha a conservação generalizada e indiferenciada de metadados pelos fornecedores de serviços para, se necessário para efeitos de prevenção, deteção e repressão de crimes graves, serem acedidos pelas autoridades competentes. Ao contrário da Diretiva, a lei nacional estipulava, ainda, regras de acesso estritas.

V. Numa perspetiva de proteção acrescida aos direitos à privacidade e à proteção de dados, a Diretiva de 2006 foi declarada inválida no Ac. *Digital Rights Ireland*, tendo o TJUE entendido que os metadados não podiam ser conservados de forma geral e indiferenciada. Contudo, o facto de não se preverem critérios objetivos que limitassem o acesso concorreu, igualmente, para a invalidade. Nos Acs. posteriores, verifica-se uma reorientação de posição, no sentido de que a conservação e o acesso são analisados separadamente.

VI. O TJUE viu-se obrigado a estabelecer exceções a este entendimento inicial, defendendo, nomeadamente, quanto aos dados de tráfego e de localização, a possibilidade de uma conservação seletiva, com base em critérios de categorias de pessoas e geográficos, e de uma conservação rápida e, quanto aos endereços IP atribuídos à fonte de uma ligação, a possibilidade de uma conservação generalizada e indiferenciada.

VII. Permanecendo a Lei n.º 32/2008 intocada ao longo de vários anos, a sua inconstitucionalidade foi, finalmente, questionada em 2022, dando origem ao Ac. do TC n.º 268/2022. Neste, o TC declarou inconstitucionais a conjugação dos seus arts. 4.º e 6.º e o seu art. 9.º. Embora fortemente influenciado pelo TJUE, a interpretação do TC apresenta diferenças importantes: a conservação e o acesso são analisados de forma separada e é o subprincípio da proporcionalidade em sentido estrito (em vez do subprincípio da necessidade) que se considera não preenchido, entendendo-se que a agressão aos direitos fundamentais dos titulares dos dados provocada pela medida de conservação dos mesmos, por abranger todas as pessoas, não é compensada pelos efeitos positivos no combate à criminalidade.

VIII. Em consequência, surgiu o Decreto da AR n.º 91/XV, sujeito, igualmente, a fiscalização de constitucionalidade, nomeadamente por não prever qualquer alteração quanto ao âmbito subjetivo da medida de conservação dos referidos dados. Por esta razão,

o TC, no Ac. n.º 800/2023, declarou inconstitucional o art. 2.º do Decreto, na parte em que (não) altera a Lei n.º 32/2008 quanto a esta questão.

IX. A vivência em comunidade impõe uma conservação generalizada e indiferenciada dos dados de tráfego e de localização, proporcional nos seguintes termos: i) sendo útil às investigações penais, é adequada às finalidades de prevenção e repressão de crimes graves; ii) impondo-se uma compreensão holística da conservação e acesso aos metadados, a adoção de regras de segurança e de acesso estritas restringe fortemente o seu potencial lesivo; iii) nenhuma das alternativas apresenta uma eficácia equivalente a esta medida; iv) a conservação seletiva coloca em causa certos princípios fundamentais, como os princípios da igualdade e da presunção da inocência; iv) sendo apenas suscetível de causar uma ingerência nos direitos fundamentais, é certamente imprescindível na investigação de certos crimes e v) sem a previsão desta medida, o princípio da proibição do défice não é garantido, deixando-se as vítimas dos crimes numa situação intolerável.

X. A Lei n.º 18/2024 procede, agora, à alteração da Lei n.º 32/2008, suprimindo as inconstitucionalidades invocadas pelo TC. Contudo, não oferece uma solução satisfatória. Quanto aos dados de tráfego e de localização (sem prejuízo dos conservados para efeitos de faturação ou por força de disposição legal especial), exclui-se a possibilidade de uma conservação generalizada e indiscriminada, prevendo-se, ao invés, uma medida de preservação de dados, de forma encapotada.

XI. A forma como o princípio da proporcionalidade é aplicado pelo TJUE não pode ser ignorada pelo TC, enquanto titular da “competência da competência” e responsável pela garantia dos direitos fundamentais dos cidadãos. A decisão de não declaração de inconstitucionalidade do Decreto da AR n.º 91/XV impunha-se, a fim de termos hoje uma resposta eficaz ao combate à criminalidade grave.

Referências

Bibliografia

ALBUQUERQUE, Paulo Pinto de, *Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, 3.^a ed., Lisboa, Universidade Católica, 2008;

BIRRER, Alena, HE, Danya, JUST, Natascha, “The state is watching you – A cross-national comparison of data retention in Europe”, in *Telecommunications Policy*, 47, Elsevier, Países Baixos, 2023;

CAMERON, Iain, “A. Court of Justice Balancing data protection and law enforcement needs: Tele2 Sverige and Watson”, in *Common Market Law Review*, 54, Kluwer Law International, Reino Unido, 2017, pp. 1467-1496;

CARDOSO, Rui, “A conservação e a utilização probatória de metadados de comunicações eletrónicas após o Acórdão do Tribunal Constitucional n.º 268/2022 – o que nasce torto...”, in *Revista do Ministério Público*, n.º 172, out.-dez. 2022, pp. 9-77;

CARNEIRO, Ana Teresa, “A inconstitucionalidade da “lei dos metadados” e o recurso extraordinário de revisão. Uma caixa de pandora?”, in *Liber Amicorum Benedita Mac Crorie*, vol. I, Braga, UMinho Editora, 2022, pp. 105-120;

CASTRO, Catarina Sarmento e, *Direito da informática, privacidade e dados pessoais*, Coimbra, Almedina, 2005;

CORREIA, João Conde, “Prova Digital: as leis que temos e a lei que devíamos ter”, in *Revista do Ministério Público*, n.º 139, jul.-set. 2014, pp. 29-59;

DIAS, Figueiredo, *Direito Processual Penal*, vol. I, Coimbra, Coimbra Editora, 1974;

FARINHO, Domingos Soares, “Comentário ao Acórdão n.º 268/2022 do Tribunal Constitucional português: a aplicação do princípio da proporcionalidade no controlo de restrições aos direitos à reserva da intimidade da vida privada e à autodeterminação informativa”, in *e-Pública - Revista Eletrónica de Direito Público*, Lisboa, vol. 10, n.º 2, 2023, pp. 206-227;

GOUVEIA, Jorge Bacelar, *Direito da Segurança: Cidadania, soberania e cosmopolitismo*, Coimbra, Almedina, 2018;

GRABOWSKA-MOROZ, Barbara, “Data Retention in the European Union”, in *European Constitutional courts towards data retention*, vol. 45, Suíça, Springer Nature Switzerland AG, 2020, pp. 3-17;

GUERRA, Clara, GALVÃO, Filipa, “Anotação ao Acórdão do Tribunal de Justiça (Grande Secção) de 8 de abril de 2014”, in *Forum de proteção de dados*, n.º 1, julho de 2015, pp. 77-80;

MACHADO, Mariana Gomes, *O acesso aos metadados pelos serviços de informações da República Portuguesa*, Coimbra, Almedina, 2019;

MEDEIROS, Rui, “Artigo 282.º”, in *Constituição Portuguesa Anotada*, Tomo III, Coimbra, Coimbra Editora, 2007, pp. 819-862;

MESQUITA, Paulo Dá, “Prolegómeno sobre prova eletrónica e interceção de telecomunicações no direito processual penal português – o Código e a Lei do Cibercrime”, in *Processo Penal, Prova e Sistema Judiciário*, 1.ª ed., Coimbra, Coimbra Editora, 2010, pp. 83-129;

MILHEIRO, Tiago Caiado, “Artigo 189.º”, in *Comentário Judiciário do Código de Processo Penal*, Tomo II – Artigos 124.º a 190.º, Coimbra, Almedina, 2019, pp. 811-847;

MIRANDA, Felipe Arady, “O direito fundamental ao livre desenvolvimento da personalidade”, in *Revista do Instituto do Direito Brasileiro*, ano 2, n.º 10, FDUL, Lisboa, pp. 11176-11211;

MIRANDA, Jorge, “Artigo 8.º”, in *Constituição da República Portuguesa*, Tomo I, 2.ª ed. revista, Lisboa, UCP Editora, 2017, pp. 120-138;

NEVES, Rita Castanheira, *As ingerências nas comunicações eletrónicas em processo penal*, Coimbra, Coimbra Editora, 2011;

NOVAIS, Jorge Reis, *Princípios Estruturantes de Estado de Direito*, Coimbra, Almedina, 2021;

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 do Ministério Público*, n.º 170, abr.-jun. 2022, pp. 9-58;

NUNES, Duarte Rodrigues, *O problema de admissibilidade dos métodos “ocultos” de investigação criminal como instrumento de resposta à criminalidade organizada*, Coimbra, Gestlegal, 2020;

NUNES, Duarte Rodrigues, *Os meios de obtenção de prova previstos na Lei do Cibercrime*, Coimbra, Gestlegal, 2018;

OJANEN, Tuomas, “Privacy Is More Than Just a Seven-Letter Word: The Court of Justice of the European Union Sets Constitutional Limits on Mass Surveillance”, in *European Constitutional Law Review*, 10, Cambridge University Press, Reino Unido, 2014, pp. 528-541;

PINHO, Carlos, “Lei de retenção de dados de comunicações eletrónicas: aposentar ou reformar?”, in *Revista do Ministério Público*, n.º 154, abr.-jun. 2018, pp. 167-192;

PINHO, Carlos, “Os problemas interpretativos resultantes da Lei n.º 32/2008, de 17 de Julho”, in *Revista do Ministério Público*, n.º 129, jan.-mar. 2012, pp. 63-93;

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*, Ano 147.º (2015) IV, Coimbra, Almedina, pp. 997-1045;

RODRIGUES, Benjamim Silva, *Da Prova Penal*, Tomo II, 1.ª Ed., Lisboa, Rei dos Livros, 2010;

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*, n.º 1, vol. 9, Brasília, Universidade de Brasília, 2017, pp. 47-68;

TELES, Miguel Galvão, “A Competência da Competência do Tribunal Constitucional”, in *Legitimidade e Legitimação da Justiça Constitucional*, Coimbra, 1995, pp. 105-125;

VENÂNCIO, Pedro Dias, *Lei do Cibercrime*, Coimbra, Coimbra Editora, 2011.

Jurisprudência

Acórdão do Supremo Tribunal de Justiça, de 07/12/2023, Proc. n.º 2766/11.3TABRR-F.S1, disponível em: <http://www.dgsi.pt>;

Acórdão do Supremo Tribunal de Justiça, de 19/12/2023, Proc. n.º 191/17.1JELSB-K.S1, disponível em: <http://www.dgsi.pt>;

Acórdão do Tribunal Constitucional n.º 232/2004, Proc. n.º 807/99, disponível em: <http://www.tribunalconstitucional.pt>;

Acórdão do Tribunal Constitucional n.º 486/2009, Proc. n.º 4/09, disponível em: <http://www.tribunalconstitucional.pt>;

Acórdão do Tribunal Constitucional n.º 403/2015, Proc. n.º 773/15, disponível em: <http://www.tribunalconstitucional.pt>;

Acórdão do Tribunal Constitucional n.º 420/2017, Proc. n.º 917/16, disponível em: <http://www.tribunalconstitucional.pt>;

Acórdão do Tribunal Constitucional n.º 464/2019, Proc. n.º 26/2018, disponível em: <http://www.tribunalconstitucional.pt>;

Acórdão do Tribunal Constitucional n.º 422/2020, Proc. n.º 528/2017, disponível em: <http://www.tribunalconstitucional.pt>;

Acórdão do Tribunal Constitucional n.º 268/2022, Proc. n.º 828/2019, disponível em: <http://www.tribunalconstitucional.pt>;

Acórdão do Tribunal Constitucional n.º 800/2023, Proc. n.º 1130/2023, disponível em: <http://www.tribunalconstitucional.pt>;

Acórdão do Tribunal da Relação de Coimbra, de 17/05/2006, Proc. n.º 1265/06, disponível em: <http://www.dgsi.pt>;

Acórdão do Tribunal da Relação de Coimbra, de 13/10/2012, Proc. n.º 84/11.6JAGRD-A.C1, disponível em: <http://www.dgsi.pt>;

Acórdão do Tribunal da Relação de Coimbra, de 26/02/2014, Proc. n.º 559/12.0GBOBR-A.C1, disponível em: <http://www.dgsi.pt>;

Acórdão do Tribunal da Relação de Coimbra, de 08/11/2017, Proc. n.º 380/17.9JACBR.C1, disponível em: <http://www.dgsi.pt>;

Acórdão do Tribunal da Relação de Coimbra, de 01/06/2022, Proc. n.º 152/21.6GGCBR-A.C1, disponível em: <http://www.dgsi.pt>;

Acórdão do Tribunal da Relação de Coimbra, de 12/10/2022, Proc. n.º 538/22.9JALRA.C1, disponível em: <http://www.dgsi.pt>;

Acórdão do Tribunal da Relação de Coimbra, de 23/11/2022, Proc. n.º 141/22.3GCLRA-A.CI, disponível em: <http://www.dgsi.pt>;

Acórdão do Tribunal da Relação de Coimbra, de 27/09/2023, Proc. n.º 13/20.6PEVIS.C1, disponível em: <http://www.dgsi.pt>;

Acórdão do Tribunal da Relação de Évora, de 27/01/2011, Proc. n.º 1276/09.3TAPTM-B.E1, disponível em: <http://www.dgsi.pt>;

Acórdão do Tribunal da Relação de Évora, de 28/02/2012, Proc. n.º 15/11.3JALRA-B.E1, disponível em: <http://www.dgsi.pt>;

Acórdão do Tribunal da Relação de Évora, de 13/11/2012, Proc. n.º 315/11.2PBPTG-A.E1, disponível em: <http://www.dgsi.pt>;

Acórdão do Tribunal da Relação de Évora, de 06/01/2015, Proc. n.º 6793/11.2TDLSB-A.E1, disponível em: <http://www.dgsi.pt>;

Acórdão do Tribunal da Relação de Évora, de 20/01/2015, Proc. n.º 648/14.6GCFAR-A.E1, disponível em: <http://www.dgsi.pt>;

Acórdão do Tribunal da Relação de Évora, de 19/05/2015, Proc. n.º 54/15.5GCBNV-A.E1, disponível em: <http://www.dgsi.pt>;

Acórdão do Tribunal da Relação de Évora, de 14/07/2020, Proc. n.º 9/20.8GAMTL-A.E1, disponível em: <http://www.dgsi.pt>;

Acórdão do Tribunal da Relação de Évora, de 22/02/2022, Proc. n.º 188/21.7GAVNO.E1, disponível em: <http://www.dgsi.pt>;

Acórdão do Tribunal da Relação de Évora, de 28/02/2023, Proc. n.º 661/17.1TELSB.E1, disponível em: <http://www.dgsi.pt>;

Acórdão do Tribunal da Relação de Guimarães, de 10/01/2005, Proc. n.º 2013/04-I, disponível em: <http://www.dgsi.pt>;

Acórdão do Tribunal da Relação de Guimarães, de 02/05/2023, Proc. n.º 12/23.6PBGMR-A.G1, disponível em: <http://www.dgsi.pt>;

Acórdão do Tribunal da Relação de Lisboa, de 10/12/2003, Proc. n.º 8673/2003-3, disponível em: <http://www.dgsi.pt>;

Acórdão do Tribunal da Relação de Lisboa, de 23/06/2004, Proc. n.º 5845/2004-3, disponível em: <http://www.dgsi.pt>;

Acórdão do Tribunal da Relação de Lisboa, de 22/01/2013, Proc. n.º 581/12.6PLSNT-A.L1-5, disponível em: <http://www.dgsi.pt>;

Acórdão do Tribunal da Relação de Lisboa, de 19/06/2014, Proc. n.º 1695/09.5PJLSB.L1-9, disponível em: <http://www.dgsi.pt>;

Acórdão do Tribunal da Relação de Lisboa, de 03/05/2016, Proc. n.º 73/16.4PFCSC-A.L1-5, disponível em: <http://www.dgsi.pt>;

Acórdão do Tribunal da Relação de Lisboa, de 28/11/2018, Proc. n.º 8617/17.8T9LSB-A.L1-3, disponível em: <http://www.dgsi.pt>;

Acórdão do Tribunal da Relação de Lisboa, de 26/01/2023, Proc. n.º 849/20.8PBCSC.L1-9, disponível em: <http://www.dgsi.pt>;

Acórdão do Tribunal da Relação de Lisboa, de 11/10/2023, Proc. n.º 1232/19.3PBFUN.L1-3, disponível em: <http://www.dgsi.pt>;

Acórdão do Tribunal da Relação do Porto, de 07/07/2016, Proc. n.º 2039/14.0JAPRT.P1, disponível em: <http://www.dgsi.pt>;

Acórdão do Tribunal da Relação do Porto, de 22/02/2021, Proc. n.º 42003/20.8YIPRT-A.P1, disponível em: <http://www.dgsi.pt>;

Acórdão do Tribunal da Relação do Porto, de 07/12/2022, Proc. n.º 5011/22.2JAPRT-A.P1, disponível em: <http://www.dgsi.pt>;

Acórdão do Tribunal da Relação do Porto, de 18/01/2023, Proc. n.º 47/22.6PEPRT-P.P1, disponível em: <http://www.dgsi.pt>;

Acórdão do Tribunal da Relação do Porto, de 01/02/2023, Proc. n.º 2748/22.0JAPRT-A.P1, disponível em: <http://www.dgsi.pt>;

Acórdão do Tribunal de Justiça da União Europeia, *Roquette Frères*, de 15/10/1980, Proc. C-145/79, disponível em: https://curia.europa.eu/jcms/jcms/j_6/pt/;

Acórdão do Tribunal de Justiça da União Europeia, *Volker und Markus Schecke*, de 09/11/2010, Procs. C-92/09 e C-93/09, disponível em: https://curia.europa.eu/jcms/jcms/j_6/pt/;

Acórdão do Tribunal de Justiça da União Europeia, *Digital Rights Ireland*, de 08/04/2014, Procs. C-293/12 e C-594/12, disponível em: https://curia.europa.eu/jcms/jcms/j_6/pt/;

Acórdão do Tribunal de Justiça da União Europeia, *Tele 2*, de 21/12/2016, Procs. C-203/15 e C-698/15, disponível em: https://curia.europa.eu/jcms/jcms/j_6/pt/;

Acórdão do Tribunal de Justiça da União Europeia, *Ministerio Fiscal*, de 02/10/2018, Proc. C-207/16, disponível em: https://curia.europa.eu/jcms/jcms/j_6/pt/;

Acórdão do Tribunal de Justiça da União Europeia, *La Quadrature du Net*, de 06/10/2020, Procs. C-511/18 e C-512/18 e C-520/18, disponível em: https://curia.europa.eu/jcms/jcms/j_6/pt/;

Acórdão do Tribunal de Justiça da União Europeia, *Prokuratuur*, de 02/03/2021, Proc. C-746/18, disponível em: https://curia.europa.eu/jcms/jcms/j_6/pt/;

Acórdão do Tribunal de Justiça da União Europeia, *Commissioner of An Garda Síochána*, de 05/04/2022, Proc. 140/20, disponível em: https://curia.europa.eu/jcms/jcms/j_6/pt/;

Acórdão do Tribunal de Justiça da União Europeia, *SpaceNet*, de 20/09/2022, Procs. C-793/19 e C-794/19, disponível em: https://curia.europa.eu/jcms/jcms/j_6/pt/;

Acórdão do Tribunal Europeu dos Direitos Humanos, *Breyer*, de 30/01/2020, Proc. C-582/14, disponível em: <https://eur-lex.europa.eu/homepage.html>;

Decisão do *Conseil d'État*, n.º 393099, de 21/04/2021, disponível em: <https://www.conseil-etat.fr>.

Legislação

Carta dos Direitos Fundamentais da União Europeia (2016/C 202/02), de 7 de junho de 2016, disponível em: <https://eur-lex.europa.eu/homepage.html>;

Code d'instruction criminelle, de 17/11/1808, disponível em: https://www.ejustice.just.fgov.be/cgi_loi/loi.pl;

Código de Processo Penal, Decreto-Lei n.º 48/95, de 15 de março, disponível em: <https://www.pgdlisboa.pt/home.php>;

Constituição da República Portuguesa, Decreto de 10 de abril de 1976, disponível em: <https://www.pgdlisboa.pt/home.php>;

Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, disponível em: <https://eur-lex.europa.eu/homepage.html>;

Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de Março de 2006, disponível em: <https://eur-lex.europa.eu/homepage.html>;

Lei n.º 23/96, de 26 de julho, disponível em: <https://www.pgdlisboa.pt/home.php>;

Lei n.º 41/2004, de 18 de agosto, disponível em: <https://www.pgdlisboa.pt/home.php>;

Lei n.º 48/2007, de 29 de agosto, disponível em: <https://www.pgdlisboa.pt/home.php>;

Lei n.º 32/2008, de 17 de julho, disponível em: <https://www.pgdlisboa.pt/home.php>;

Lei n.º 109/2009, de 15 de setembro, disponível em: <https://www.pgdlisboa.pt/home.php>;

Lei n.º 62/2013, de 26 de agosto, disponível em: <https://www.pgdlisboa.pt/home.php>;

Lei n.º 18/2024, de 5 de fevereiro, disponível em: <https://www.pgdlisboa.pt/home.php>;

Portaria n.º 694/2010, de 16 de agosto, disponível em: <https://www.pgdlisboa.pt/home.php>;

Regulamento Geral de Proteção de Dados, 2016/679, de 27 de abril de 2016, disponível em: <https://eur-lex.europa.eu/homepage.html>.

Outros

BERTHÉLÉMY, Chloé, *Europe's data retention saga and its risks for digital rights*, de 02/09/2021, disponível em: <https://edri.org/our-work/europes-data-retention-saga-and-its-risks-for-digital-rights/>;

BREYER, Patrick, *Conservation “ciblée” des données : cartographier ce que le gouvernement belge veut cacher*, de 08/06/2022, disponível em: <https://www.patrick-breyer.de/en/conservation-ciblee-des-donnees-cartographier-ce-que-le-gouvernement-belge-veut-cacher/>;

Chambre des représentants, Projet de Loi relatif à la collecte et à la conservation des données d'identification et des métadonnées dans le secteur des communications électroniques et à la fourniture de ces données aux autorités, de 17/03/2022, disponível em: <https://www.lachambre.be/FLWB/PDF/55/2572/55K2572001.pdf>;

Comissão Europeia, *Relatório de Avaliação sobre a Directiva relativa à conservação de dados (2006/24/CE)*, Bruxelas, 2011, disponível em: <https://eur-lex.europa.eu/homepage.html>;

Comunicado de Imprensa n.º 54/14, de 08/04/2014, relativo ao Acórdão *Digital Rights Ireland Ltd*, disponível em: https://curia.europa.eu/jcms/jcms/j_6/pt/;

Conclusões do Advogado-Geral Henrik Saugmandsgaard Øe, 19 de julho de 2016, disponível em: <https://eur-lex.europa.eu/homepage.html>;

Contratos de adesão da Vodafone, disponível em: <https://www.vodafone.pt/content/dam/digital-sites/downloads/formularios/particulares/portabilidade-movel.pdf>;

Contrato de adesão da NOS, disponível em: https://www.nos.pt/content/dam/nos/assets/pdfs/Proposta_de_subscricao.pdf;

Decreto da Assembleia da República n.º 91/XV, de 13/10/2023, disponível em: <https://www.parlamento.pt>;

Deliberação da Comissão Nacional de Proteção de Dados n.º 641/2007, de 09/05/2017, disponível em: <https://www.cnpd.pt>;

Deliberação da Comissão Nacional de Proteção de Dados n.º 1008/2017, de 18/07/2017, disponível em: <https://www.cnpd.pt>;

European Commission, Commission Staff Working Document – Annex to the Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC, “Data Preservation versus Data Retention”, 2005, disponível em: <https://eur-lex.europa.eu/homepage.html>;

European Commission, Directorate-General For Migration And Home Affairs, DUPONT, Claire, CILLI, Valentina, et al., Study on the retention of electronic communications non-content data for law enforcement purposes – Final report, Publications Office, 2020;

FIDALGO, Sónia, “Conservação de Metadados – O Acórdão n.º 268/2022”, in *Revista Portuguesa de Direito Constitucional*, n.º 3, 2023, p. 56, disponível em: <https://rpdc.pt>;

LUND, Jesper, *The new Danish data retention law: attempts to make it legal failed after just six days*, de 15/06/2022, disponível em: <https://itpol.dk/articles/new-Danish-data-retention-law-2022>;

LYSKEY, Orla, *Tele2 Sverige AB and Watson et al: Continuity and Radical Change*, de 12/01/2017, disponível em: <https://europeanlawblog.eu/2017/01/12/tele2-sverige-ab-and-watson-et-al-continuity-and-radical-change/>;

Nota Prática da Procuradoria-Geral da República n.º 1/2012, *O endereço IP e a identificação do seu utilizador*, disponível em: [https://cibercrime.ministeriopublico.pt/notas-praticas](https://cibercrime.ministeriopublico.pt/notas-praticas;);

Nota Prática da Procuradoria-Geral da República n.º 2/2013, *A obtenção do endereço IP – súmula da jurisprudência recente*, de 03/04/2013, disponível em: [https://cibercrime.ministeriopublico.pt/notas-praticas](https://cibercrime.ministeriopublico.pt/notas-praticas;);

Nota Prática da Procuradoria-Geral da República n.º 7/2015, de 30/12/2015, *Retenção de dados de tráfego e Lei n.º 32/2008, de 17 de Julho*, disponível em: [https://cibercrime.ministeriopublico.pt/notas-praticas](https://cibercrime.ministeriopublico.pt/notas-praticas;);

Nota Prática da Procuradoria-Geral da República n.º 8/2016, de 18/02/2016, *Pedido de dados a operadoras de comunicações*, disponível em: [https://cibercrime.ministeriopublico.pt/notas-praticas](https://cibercrime.ministeriopublico.pt/notas-praticas;);

Parecer do Conselho Consultivo da Procuradoria-Geral da República n.º 16/1994, de 07/07/1994, disponível em: [https://www.ministeriopublico.pt/pareceres-pgr](https://www.ministeriopublico.pt/pareceres-pgr;);

Parecer da Comissão Nacional de Proteção de Dados n.º 38/2017, Proc. n.º 8243/2017, de 30/05/2017, disponível em: [https://www.cnpd.pt](https://www.cnpd.pt;);

Parecer da Comissão Nacional de Proteção de Dados n.º 2022/50, de 21/06/2022, disponível em: [https://www.cnpd.pt](https://www.cnpd.pt;);

Proposta de Regulamento do Parlamento Europeu e do Conselho relativo ao respeito pela vida privada e à proteção de dados pessoais nas comunicações eletrónicas e que revoga a Diretiva 2002/58/CE, de 10/01/2017, disponível em: <https://eur-lex.europa.eu/homepage.html>;

Proposta de Lei n.º 109/X, de 16/11/2006, disponível em: [https://www.parlamento.pt](https://www.parlamento.pt;);

Projeto de Lei n.º 70/XV/1ª (Partido Social Democrata), de 11/05/2022, disponível em: [https://www.parlamento.pt](https://www.parlamento.pt;);

Projeto de Lei n.º 79/XV/1ª (CHEGA), de 19/05/2022, disponível em: <https://www.parlamento.pt>;

Projeto de Lei n.º 100/XV/1ª (Partido Comunista Português), de 27/05/2022, disponível em: <https://www.parlamento.pt>;

Proposta de Lei n.º 11/XV/1ª, de 26/05/2022, disponível em: <https://www.parlamento.pt>;

Relatório de informação n.º 110 (2023-2024), Comissão do Senado Francês, 15/11/2023, disponível em: <https://www.senat.fr/rap/r23-110/r23-110.html>;

Relatório Sueco, *Datalagring och åtkomst till elektronisk information*, Estocolmo, 2023, disponível em: <https://www.regeringen.se>;

TOKMETZIS, Dimitri, *How your innocent smartphone passes on almost your entire life to the secret service*, 2014, disponível em: https://netzpolitik.org/wp-upload/bits_of_freedom_on_the_metadata_of_your_phone.pdf.