CNPD
Comissão Nacional
de Proteção de Dados

PARECER/2022/50

I. Pedido

1. A Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias, da Assembleia da República, submeteu à Comissão Nacional de Proteção de Dados (doravante CNPD), para parecer, Proposta de Lei n.º 11/XV/1.ª (GOV), que *«regula o acesso a metadados referentes a comunicações eletrónicas para fins de investigação criminal»*.

2. A CNPD emite parecer no âmbito das suas atribuições e competências enquanto autoridade administrativa independente com poderes de autoridade para o controlo dos tratamentos de dados pessoais, conferidos pela alínea *c)* do n.º 1 do artigo 57.º, conjugado com a alínea *b)* do n.º 3 do artigo 58.º, e com o n.º 4 do artigo 36.º, todos do Regulamento (UE) 2016/679, de 27 de abril de 2016 – Regulamento Geral sobre a Proteção de Dados (doravante, RGPD), em conjugação com o disposto no artigo 3.º, no n.º 2 do artigo 4.º, e na alínea *a)* do n.º 1 do artigo 6.º, todos da Lei n.º 58/2019, de 8 de agosto, que executa na ordem jurídica interna o RGPD.

II. Análise

3. De acordo com o artigo 1.º da presente Proposta de Lei, esta «*estabelece as regras de acesso, para fins de investigação criminal, a dados tratados pelas empresas que oferecem redes e ou serviços de comunicações eletrónicas*» e «*procede à segunda alteração à Lei n.º 41/2004, de 18 de agosto, alterada pela Lei n.º 46/2012, de 29 de agosto* [...]».

4. Compreendendo-se a necessidade de acesso a dados pessoais de tráfego e de localização para a investigação e repressão criminal, a CNPD saúda a intenção de encontrar um prudente equilíbrio entre, por um lado, o interesse público de segurança e paz públicas e, por outro lado, os direitos fundamentais ao respeito pela vida privada, à autodeterminação informativa e ao livre desenvolvimento da personalidade.

5. Em especial, acompanha-se a preocupação manifestada, na exposição de motivos da Proposta de Lei, com os crimes graves e violentos cometidos pelas organizações criminosas que, como aí se sublinha, «*recorrem frequentemente à Internet (nomeadamente à* dark web*) e às telecomunicações móveis, sob encriptação e possível anonimato*». O que não pode deixar de se notar é que para monitorizar as comunicações e recolher prova no contexto da *dark web* o regime apresentado nesta Proposta de Lei de pouco ou nada serve, porque é a natureza da *dark web* que, precisamente, impede a identificação do destino do acesso, razão pela qual é necessária a utilização de um *software/browser* para mascarar as comunicações. Não se percebe, por isso, por que se invoca a *dark web* para motivar a previsão de um regime de acessos a dados pessoais em sede de comunicações eletrónicas que, claramente, não permite a monitorização das comunicações; de resto

como a Lei n.º 32/2008, de 17 de julho, não terá também permitido. O mesmo raciocínio vale para a referência à utilização de tecnologias de encriptação.

6. Ainda a propósito da exposição de motivos, sublinha-se que existe já um regime legal referente à recolha e conservação de prova em relação a crimes cometidos por meio de sistema informático – Lei do Cibercrime (Lei n.º 109/2009, de 15 de setembro, alterada pela Lei n.º 79/2021, de 14 de novembro) – pelo que também por este motivo o teor desta proposta de lei não aparenta encontrar fundamento.

7. De todo modo, na análise do regime de acesso a dados pessoais relativos a comunicações eletrónicas aqui proposto e da sua conformidade com a Constituição da República Portuguesa (CRP) e a Carta dos Direitos Fundamentais da União Europeia (Carta), a CNPD pautar-se-á especialmente pelos argumentos, condições e limites explicitados pelo Tribunal Constitucional (TC) no acórdão 268/2022, de 19 de abril de 2022[1], bem como nos acórdãos do Tribunal de Justiça da União Europeia (TJUE) *Digital Rights Ireland*[2], *Tele 2*[3] e *La Quadrature du Net*[4].

8. Tendo em conta a referida jurisprudência, começa-se por saudar a opção de criar um regime legal que não prevê a conservação generalizada de dados pessoais relativos ao tráfego e à localização para a finalidade de investigação e repressão criminais.

9. E assinala-se que a previsão, para a finalidade de investigação criminal, de acesso a dados pessoais de tráfego conservados pelas operadoras de comunicações eletrónicas para efeitos de faturação não suscita, de per si, reservas. A finalidade de investigação e repressão criminal é em si mesma uma finalidade de interesse público que pode legitimar a reutilização de dados pessoais, desde que o acesso se revele adequado, necessário e não excessivo face a tal finalidade.

10. No entanto, algumas das soluções propostas contrariam o sentido da jurisprudência acima citada, diminuindo as garantias dos direitos fundamentais dos cidadãos. É sobre este ponto que incide o essencial da apreciação da CNPD.

i. A diminuição das garantias fundamentais dos cidadãos

11. Em primeiro lugar, destaca-se que com esta Proposta de Lei não é alcançado o objetivo declarado de assegurar um «prudente equilíbrio» entre, por um lado, o interesse público de segurança e paz públicas que justifica dotar os órgãos de polícia criminal e as autoridades judiciárias de meios de investigação e de prova

[1] Cf. https://dre.pt/dre/detalhe/acordao-tribunal-constitucional/268-2022-184356510
[2] Acórdão de 8 de abril de 2014, procs. C-293/12 e C-594/12.
[3] Acórdão de 21 de dezembro de 2016, procs. C-203/15 e C-698/15.
[4] Acórdão de 6 de outubro de 2020, procs. C-511/18, C-512/18 e C-520/18.

adequados e, por outro lado, os direitos fundamentais de cada cidadão, máxime do respeito pela vida privada e familiar, à autodeterminação informativa e ao livre desenvolvimento da personalidade.

12. Na verdade, na presente Proposta de Lei, há uma redução acentuada das garantias dos direitos fundamentais dos cidadãos, por comparação com o regime jurídico anterior de conservação e transmissão de dados pessoais relativos a comunicações eletrónicas, seja o que se encontrava previsto na Lei n.º 32/2008, de 17 de julho (sobre retenção dos dados relativos às comunicações eletrónicas), seja o que se encontra ainda previsto na Lei do Cibercrime.

13. Essa diminuição da tutela dos direitos fundamentais causa a maior perplexidade, sobretudo tendo em conta o contexto em que a Proposta de Lei surge: após a declaração pelo TC da inconstitucionalidade com força obrigatória geral do regime legal de retenção de dados relativos às comunicações eletrónicas, que não oferecia garantias adequadas à proteção daqueles direitos fundamentais, e após sucessivas decisões do TJUE a assinalar a violação desproporcionada dos direitos fundamentais pelo regime da União e por regimes legais nacionais de conservação e acesso a dados pessoais relativos às comunicações eletrónicas.

14. Acresce que essa diminuição das garantias não ocorre apenas quanto a um único aspeto de regime, antes se concretizando em diferentes planos, criando uma teia estranguladora dos direitos e liberdades fundamentais. Vejamos.

a. *O acesso pelas autoridades judiciárias*

15. A diminuição das garantias fundamentais ocorre, desde logo, no plano da legitimidade e controlo do acesso aos dados pessoais relativos a comunicações eletrónicas para a finalidade de investigação e repressão criminal.

16. Enquanto na Lei n.º 32/2008, de 17 de julho, no n.º 2 do artigo 3.º e no artigo 9.º, se faz depender o acesso pelas autoridades competentes (*i.e.*, autoridades judiciárias e autoridades de polícia criminal) de despacho do juiz de instrução, a ordenar ou autorizar a transmissão dos dados, agora, nesta Proposta, as autoridades judiciárias (portanto, também o Ministério Público, e os órgãos de polícia criminal, por delegação de competências genéricas, ao abrigo da Diretiva 1/2002, de 4 de abril, da Procuradoria-Geral da República[5]) podem aceder sem prévio despacho do juiz de instrução aos dados pessoais – cf. artigos 2.º e 3.º, n.º 1, da Proposta de Lei. Aliás, em ponto algum, se prevê a necessidade de intervenção do juiz de instrução.

[5]Acessível em https://files.dre.pt/2s/2002/04/079000000/0622106224.pdf

17. De resto, nem sequer se impõe na Proposta de Lei o dever de fundamentação circunstanciada do pedido de acesso aos dados, como se encontra previsto no n.º 1 do artigo 9.º da Lei n.º 32/2008.

18. A este propósito, cumpre recordar que, de acordo com o n.º 4 do artigo 32.º da CRP, «*[t]oda a instrução é da competência de um juiz, o qual pode, nos termos da lei, delegar noutras entidades a prática dos actos instrutórios que se não prendam directamente com os direitos fundamentais*».

19. Tendo em conta que o acesso aos dados pessoais relativos a comunicações eletrónicas, máxime, aos dados de tráfego e de localização, implica uma restrição considerável dos direitos à autodeterminação informativa e ao respeito pela vida privada e, em especial, à liberdade e ao livre desenvolvimento da personalidade, consagrados nos artigos 26.º e 35.º da CRP, a ausência de previsão de controlo pelo juiz de instrução do acesso a tais dados tem direto impacto para estes direitos fundamentais e significa um retrocesso na sua tutela[6].

20. Repare-se que mesmo no domínio da Lei do Cibercrime, onde as autoridades judiciárias estão legitimadas a aceder aos dados ou ordenar esse acesso, salvaguarda-se a intervenção do juiz sempre que os dados recolhidos possam pôr em causa a privacidade do arguido ou de terceiros, sob pena de nulidade das provas recolhidas (cf. n.º 3 do artigo 16.º da Lei do Cibercrime).

21. Esta opção legislativa é, pois, de duvidosa constitucionalidade, e suscita a maior perplexidade sobretudo quando a jurisprudência do TJUE e do TC tem persistentemente sublinhado a importância, no juízo de proporcionalidade da restrição aos direitos fundamentais por força do acesso a dados relativos às comunicações eletrónicas, da previsão legal de intervenção prévia do juiz.

22. Aliás, o Tribunal Europeu dos Direitos Humanos (TEDH), no acórdão *Big Brother Watch*[7], estende os pressupostos de uma legítima interceção de comunicações eletrónicas à operação de acesso aos dados relativos às comunicações eletrónicas (cf. § 507). Assim, e como sintetiza o TC no acórdão 464/2019, de 21 de outubro, o TEDH estabelece os seguintes critérios de conformidade destas medidas com o direito ao respeito pela vida privada e familiar: «*(1) o regime deve estar de acordo com a lei, no sentido de esta ser clara, acessível e de efeitos previsíveis para os cidadãos; (2) deve prosseguir um objetivo legítimo, (3) e ser necessário numa sociedade democrática, restringindo-se ao combate à criminalidade grave; (4) o acesso deve estar sujeito*

[6] A CNPD mantém o entendimento, por si explanado em anteriores pareceres sobre esta matéria, de que o acesso aos dados de tráfego e de localização afeta o conteúdo do direito fundamental à inviolabilidade das comunicações eletrónicas, consagrado no artigo 34.º da CRP. Não obstante, para maior clareza da exposição em coerência com o recente acórdão do TC, a CNPD opta por não focar, neste parecer, a restrição desse direito fundamental.

[7] Acórdão de 25 de maio de 2021, queixas n.º 58170/13, 62322/14 e 24960/15.

a uma autorização prévia decidida por um tribunal ou por uma entidade administrativa independente; (5) a lei deve providenciar garantias adequadas contra a arbitrariedade».

23. A exigência de uma autorização prévia por um tribunal ou por uma entidade administrativa independente implica que a necessidade (e a proporcionalidade *stricto sensu*) do acesso a tais dados seja avaliada por uma autoridade que não esteja diretamente envolvida na investigação, portanto, que não seja aquela que pretende aceder aos dados ou que dirige a investigação. Donde a imprescindibilidade de uma intervenção do juiz neste procedimento.

24. Por tudo isto, a CNPD recomenda a alteração dos artigos 2.º e 3.º da Proposta, no sentido de prever a necessidade de despacho autorizativo do juiz para o acesso aos dados pessoais relativos às comunicações eletrónicas.

b. O alargamento do catálogo de crimes

25. Mas a diminuição das garantias fundamentais dos cidadãos manifesta-se ainda no alargamento do catálogo de crimes que justifica o acesso aos dados pessoais de tráfego e localização.

26. Ao contrário do regime constante da Lei n.º 32/2008, de 17 de julho, que restringia a conservação e a transmissão dos dados pessoais relativos ao tráfego e localização à finalidade de investigação, deteção e repressão de crimes graves (cf. n.º 1 do artigo 1.º e do artigo 3.º, e ainda o n.º 1 do artigo 9.º), tipificados na alínea *g)* do n.º 1 do artigo 2.º, a Proposta de Lei define um regime de transmissão dos mesmos dados pessoais para a investigação e repressão dos seguintes crimes:

i. previstos nos n.ºs 1 e 2 do artigo 189.º do Código do Processo Penal (CPP), portanto, acrescendo aos crimes graves previstos na alínea *g)* do n.º 1 do artigo 2.º da Lei n.º 32/2008, os crimes puníveis com pena de prisão superior, no seu máximo, a 3 anos;

ii. os crimes previstos na Lei do Cibercrime, correspondentes a criminalidade informática com um grau de gravidade identificado por pena de prisão de máximo igual ou superior a 5 anos (pelo menos), com exceção do crime de acesso ilegítimo;

iii. «os crimes cometidos por meio de sistema informático, contanto que puníveis com pena de prisão de máximo igual ou superior a 1 ano».

27. Em suma, aos «*crimes de terrorismo, criminalidade violenta, criminalidade altamente organizada, sequestro, rapto e tomada de reféns, crimes contra a identidade cultural e integridade pessoal, contra a segurança do Estado, falsificação de moeda ou títulos equiparados a moeda e crimes abrangidos por convenção sobre segurança da navegação aérea ou marítima*» (que estavam previstos na Lei n.º 32/2008), somam-se agora os crimes do n.º 1 do artigo 187.º do CPP, onde se inserem, entre outros, os crimes puníveis com pena de prisão superior, no seu máximo, a 3 anos, bem como certos tipos de criminalidade informática, em função da respetiva moldura penal e ainda todos os demais crimes cometidos por meio de sistema informático, contanto que puníveis com pena de prisão de máximo igual ou superior a 1 ano.

28. Por outras palavras, esta Proposta de Lei alarga a finalidade do acesso a dados pessoais de tráfego e de localização, no contexto da utilização de comunicações eletrónicas, muito além do que estatuía a Lei n.º 32/2008, e também indo além do previsto na Lei do Cibercrime, inclusive para crimes cujo grau de censurabilidade é manifestamente baixo.

29. Desnecessário seria aqui recordar a relevância que a jurisprudência do TC e do TJUE tem dado, na ponderação dos direitos e interesses em tensão a propósito do acesso aos dados pessoais de tráfego e de localização, ao facto de o acesso se limitar à investigação da criminalidade grave, como indicava a Diretiva transposta pela Lei n.º 32/2008. Por exemplo, o TC, no acórdão n.º 268/2022, aqui já citado, refere "*[n]ão parecem restar dúvidas que a investigação, prevenção e repressão de crimes graves, definidos como «crimes de terrorismo, criminalidade violenta, criminalidade altamente organizada, sequestro, rapto e tomada de reféns, crimes contra a identidade cultural e integridade pessoal, contra a segurança do Estado, falsificação de moeda ou títulos equiparados a moeda e crimes abrangidos por convenção sobre segurança da navegação aérea ou marítima» (alínea g) do n.º 1 do artigo 2.º da Lei n.º 32/2008) — finalidade elencada no n.º 1 do artigo 1.º da Lei n.º 32/2008 — assume relevo constitucional, por se dirigir à salvaguarda da legalidade democrática e da ação penal. Isso mesmo, aliás, foi reconhecido no Acórdão do Tribunal Constitucional n.º 420/2017 e está em consonância com a conclusão do Tribunal de Justiça, no Acórdão Digital Rights, segundo a qual a luta contra a criminalidade grave e o terrorismo constituem objetivos de interesse geral da União (n.ºs 41 a 43)*".

30. Acrescente-se que, no acórdão *La Quadrature du Net* (ponto 167), o TJUE veio clarificar que «*os Estados-Membros têm a possibilidade de prever na sua legislação que um acesso a dados de tráfego e a dados de localização pode, no respeito dessas mesmas condições materiais e processuais, ocorrer para efeitos de luta contra a criminalidade grave ou de salvaguarda da segurança nacional quando os referidos dados são conservados por um fornecedor em conformidade com os artigos 5.º, 6.º e 9.º ou ainda com o artigo 15.º, n.º 1, da Diretiva 2002/58*».

CNPD
Comissão Nacional
de Proteção de Dados

31. Paralelamente, o TEDH exige para a restrição do direito ao respeito pela vida privada e familiar, neste contexto seja necessária numa sociedade democrática, restringindo-*se* à investigação e combate à criminalidade grave (cf. §§ 519 e 522 do Acórdão *Big Brother Watch*).

32. Nessa medida, a restrição dos direitos à reserva da vida privada, à autodeterminação informativa e à liberdade de livre desenvolvimento da personalidade que o acesso a dados de tráfego sempre representa só parece ter-se por proporcional se tiver em vista a investigação e repressão de crimes graves, não tendo sido apresentadas razões que justifiquem a extensão da restrição dos direitos fundamentais além do que já resulta do artigo 187.º do CPP e da Lei do Cibercrime.

33. A legitimação do acesso para a investigação de praticamente quaisquer crimes independentemente da sua gravidade, de per si, representa uma restrição desproporcionada dos direitos à reserva da vida privada, à autodeterminação informativa e ao livre desenvolvimento da personalidade, em violação do n.º 2 do artigo 18.º e do n.º 1 do artigo 52.º da CRP; desproporcionalidade que é acentuada pela previsão conjunta da possibilidade de acesso pelo Ministério Público sem controlo direto e prévio de um juiz, já acima assinalada.

34. Deste modo, a CNPD recomenda a eliminação da alínea *c)* do artigo 2.º da Proposta de Lei.

c. *Alargamento dos dados pessoais objeto de conservação e de acesso*

35. E, num terceiro plano, a Proposta de Lei alarga as categorias de dados pessoais objeto de conservação pelas operadoras que oferecem os serviços de rede e de comunicações eletrónicas, alterando o leque de dados pessoais previsto na Lei n.º 41/2004, de 18 de agosto, alterada pela Lei n.º 46/2012, de 29 de agosto – Lei da Privacidade nas Comunicações Eletrónicas.

36. Na verdade, sob o pretexto de uma atualização dos dados de identificação dos equipamentos utilizados, o artigo 8.º da Proposta de Lei altera o n.º 2 do artigo 6.º da Lei n.º 41/2004.

37. Antes de mais, reitera-se que a previsão de acesso para a finalidade de investigação criminal a dados pessoais de tráfego conservados pelas operadoras de comunicações eletrónicas para efeito de faturação não suscita, de per si, reservas. A finalidade de investigação e repressão criminal é em si mesma uma finalidade de interesse público que pode legitimar a reutilização de dados pessoais, desde que o acesso se revele adequado, necessário e não excessivo face a tal finalidade.

38. O que já suscita as maiores reservas é a previsão legal de recolha e conservação pelas operadoras de comunicações eletrónicas de dados pessoais que não sejam demonstradamente necessários para a finalidade de faturação, mas com a aparência do seu enquadramento nessa finalidade.

39. De facto, ao leque dos dados de identificação do assinante e do equipamento (dados de base) inicialmente previstos no n.º 2 do artigo 6.º da Lei n.º 41/2004, introduz-se agora, na alínea *a)*, vários dados, de que se destaca o IMSI (identidade internacional do assinante móvel) e o IMEI (identidade internacional do equipamento móvel). E aqui, sem especificar se o IMSI e o IMEI são apenas os do assinante.

40. E, ao leque de dados de tráfego previstos nas alíneas *b)* e *c)* do n.º 2 do artigo 6.º – *«número total de unidades a cobrar para o período de contagem, bem como o tipo, hora de início e duração das chamadas efetuadas ou o volume de dados transmitidos»* e *«data da chamada ou serviço e número chamado»*, respetivamente –, junta-se agora os dados relativos a *«grupo data/hora associado»* (cf. a redação da alínea *c)* do n.º 2 do artigo 6.º agora proposta).

41. Acresce que, no que diz respeito aos dados de tráfego relativos ao acesso à Internet, se acrescenta *«número de telefone, endereço de protocolo IP utilizado para estabelecimento de comunicação, porto de origem de comunicação, bem como os dados associados ao início e fim do acesso à Internet»* (cf. nova alínea *d)* introduzida pela Proposta no n.º 2 do artigo 6.º).

42. Ora, entre este novo elenco de dados pessoais relativos às comunicações eletrónicas que se pretende introduzir no n.º 2 do artigo 6.º da Lei n.º 41/2004, apresentam-se dados cuja previsão legal é, *prima facie*, desnecessária.

43. É, desde logo, o que sucede com alguns dados cuja inserção se afigura redundante, por já estarem previstos no n.º 2 do artigo 6.º na sua redação atual: o *número de telefone*, previsto na nova alínea *d)*, por já estar compreendido nos dados de identificação elencados na alínea *a);* e os dados relativos ao *grupo data/hora associado,* uma vez que, se bem se interpreta esta expressão, tais dados estão já previstos nas atuais alíneas *b)* e *c)* do referido preceito (especificamente, *«tipo, hora de início e duração das chamadas efetuadas»* e *«data da chamada»*).

44. Mas há outros dados cuja inserção naquela norma se revelam mesmo desnecessários para a finalidade de faturação, não sendo por isso admissível a sua previsão nesta sede. É manifestamente esse o caso dos dados de tráfego, previstos na nova alínea *d),* relativos ao *início e fim do acesso à Internet*: a *«conservação do volume de dados transmitidos»* (prevista já na alínea *b)* do n.º 2 do artigo 6.º da Lei n.º 41/2004) parece ser suficiente para efeito de faturação, não sendo necessário conhecer o início e fim desse acesso.

45. Quanto à previsão da recolha do IMEI, na nova redação proposta para a alínea *a)* do n.º 2 do artigo 6.º, não se discutindo aqui a necessidade do seu tratamento no contexto da execução do contrato de prestação do serviço de comunicações eletrónicas, sobra a dúvida séria quanto à sua necessidade para efeito de

faturação ou de pagamento dos serviços prestados, que é, recorda-se, a finalidade para a qual o n.º 2 do artigo 6.º da Lei n.º 41/2004 admite a conservação de dados de tráfego.

46. Não estando demonstrada a necessidade de tais dados pessoais para essa específica finalidade de faturação, qualquer norma legal que preveja a sua recolha e conservação para essa mesma finalidade representa uma restrição desproporcionada dos direitos fundamentais ao respeito pela vida privada e familiar, ao livre desenvolvimento da personalidade e de autodeterminação informativa, em violação do n.º 2 do artigo 18.º da CRP e do n.º 1 do artigo 52.º da Carta, e especificamente do princípio da minimização dos dados, consagrado na alínea *c)* do n.º 1 do artigo 5.º do RGPD.

47. Afigura-se, com isto, estar a impor-se, de forma encapotada, a conservação dos dados pessoais para fins de investigação criminal, sob a aparência de dados necessários à faturação dos serviços de comunicações eletrónicas prestados.

48. Repare-se que da jurisprudência do TC não resulta a impossibilidade de o legislador nacional impor às operadoras de comunicações eletrónicas a conservação generalizada de «dados base» dos seus clientes (conforme o conceito adotado por esse tribunal) para a finalidade de investigação criminal – aqui se compreendendo que «*[o]s dados de base referem-se à conexão à rede, independentemente de qualquer comunicação, permitindo a identificação do utilizador de certo equipamento — nome, morada, número de telefone*» (cf. ponto 6.1. do acórdão n.º 268/2022). Na medida em que se entender e demonstrar ser adequado e necessário para a investigação criminal a conservação de dados de identificação do equipamento mais detalhados do que aqueles que são necessários à faturação e pagamento dos serviços de comunicações eletrónicas, nada obsta, pois, a que o legislador nacional o preveja com esse específico fundamento[8]. Mas a presente Proposta de Lei não assume tal intenção, antes considerando tais dados como justificados no contexto da faturação e pagamento de serviços de comunicação eletrónica, sem, contudo, demonstrar a necessidade dos mesmo para essa mesma finalidade.

49. De resto, tudo o que se insira já no conceito de dados de tráfego – «*os dados funcionais necessários ao estabelecimento de uma ligação ou comunicação e os dados gerados pela utilização da rede (por exemplo, localização do utilizador, localização do destinatário, duração da utilização, data e hora, frequência)* [...c]*onstituem, pois, elementos já inerentes à própria comunicação, na medida em que permitem identificar, em*

[8] Cf. pontos 17.1. e 17.2 do acórdão do TC n.º 268/2022; e pontos 152-159 do acórdão *La Quadrature do Net* do TJUE, que, no essencial, admite *para efeitos da salvaguarda da segurança nacional, da luta contra a criminalidade grave e da prevenção de ameaças graves contra a segurança pública, uma conservação generalizada e indiferenciada dos endereços IP atribuídos à fonte de uma ligação, por um período temporalmente limitado ao estritamente necessário;* e, para efeitos da luta contra a criminalidade (não grave) e da salvaguarda da segurança pública, *uma conservação generalizada e indiferenciada de dados relativos à identidade civil dos utilizadores de meios de comunicações eletrónicos*.

tempo real ou a posteriori, os utilizadores, o relacionamento direto entre uns e outros através da rede, a localização, a frequência, a data, hora e a duração da comunicação [...]» (cf. ponto 6.1. do acórdão do TC n.º 268/2022) – já só pode ser objeto de conservação na estrita medida da sua necessidade no contexto da faturação e pagamento de serviços de comunicação eletrónica; sendo certo que para certos serviços (de valor acrescentado), a Lei n.º 41/2004 exige mesmo o consentimento do titular dos dados.

50. Assim, é desproporcionada, em violação do n.º 2 do artigo 18.º da CRP e do n.º 1 do artigo 52.º da Carta, por não estar demonstrada a necessidade do seu tratamento para a finalidade de faturação e pagamento dos serviços de comunicações, a previsão legal da conservação dos dados de tráfego *associados ao início e fim do acesso* à Internet, recomendando-se, por isso, a sua eliminação da alínea *d)* do n.º 2 do artigo 6.º da Lei n.º 41/2004, na redação proposta.

51. Recomenda-se ainda a eliminação dos dados relativos a *número de telefone* e *grupo data/hora associado* (cf. alíneas *c)* e *d)* do n.º 2 do artigo 6.º, na redação agora proposta), pela sua redundância em relação aos dados já previstos na atual versão deste artigo.

ii. O direito de informação dos respetivos titulares

52. A Proposta de Lei prevê ainda, no artigo 3.º, o dever de notificação dos titulares dos dados.

53. Quanto à garantia dos direitos dos titulares dos dados, máxime o direito de informação que o TC destacou, em linha com a jurisprudência do TJUE (cf. Acórdão Tele 2, ponto 121) e do Tribunal Europeu dos Direitos Humanos (TEDH) – em especial, acórdão *Big Brother Watch*[9] – a Proposta vem prever o dever de a autoridade judiciária proceder a tal notificação, no despacho em que determina a solicitação dos dados, salvo se o Ministério Publico, em inquérito, considerar que a notificação pode pôr em causa a investigação, dificultar a descoberta da verdade ou criar perigo para a vida, para a integridade física ou psíquica ou para a liberdade dos participantes processuais, das vítimas do crime ou de outras pessoas, caso em que tal notificação pode ser protelada, nos termos previstos no n.º 2 do artigo 3.º.

54. Além de não se perceber a razão porque esta faculdade de protelamento não vem especificada também para o juiz, sublinha-se que, estendendo-se essa notificação aos titulares dos dados transmitidos, tal implica a notificação não apenas às pessoas singulares objeto de investigação, mas também a todas as pessoas singulares com quem tenha havido comunicação ou tentativa de comunicação, o que aumenta significativamente o universo de titulares de dados a notificar.

[9] Acórdão de 25 de maio de 2021, queixas n.º 58170/13, 62322/14 e 24960/15.

iii. Destruição de dados

55. O regime de destruição de dados, previsto no artigo 5.º da Proposta, suscita dúvidas quanto ao seu real alcance. Sobretudo quando comparado com o regime previsto no artigo 11.º da Lei n.º 32/2008. Aí se previa a eliminação dos dados, por ordem do juiz dirigida às autoridades competentes pela investigação criminal, logo que não fossem mais necessários, especificando-se que tal sucederia em caso de arquivamento definitivo do processo penal, absolvição ou condenação transitadas em julgado, prescrição do procedimento penal e amnistia. Agora, propõe-se a eliminação apenas se não servirem de meio de prova após o transito em julgado da decisão que puser termo ao processo.

56. Não se alcança a intenção desta disposição, admitindo-se poder haver confusão entre a conservação de dados no contexto do processo-crime e a conservação de dados no contexto da investigação criminal pelas autoridades competentes.

57. A imposição da destruição dos dados, depois de transitada em julgado a decisão, apenas se aqueles não tiverem servido de meio de prova revela-se proporcional no contexto específico do processo criminal; já quanto aos dados conservados pelas autoridades competentes para a investigação criminal será manifestamente desproporcionada a previsão da sua destruição apenas naquela circunstância. Na verdade, estando os dados integrados no processo criminal, afigura-se adequado e proporcional que a sua conservação por aquelas autoridades cesse nas circunstâncias elencadas no artigo 11.º da Lei n.º 32/2008.

58. Recomenda-se, por isso, a clarificação do artigo 5.º da Proposta, quanto ao seu âmbito de aplicação, sugerindo-se a reprodução do teor do artigo 11.º da Lei n.º 32/2008.

iv. A competência para regulamentar o novo regime de acesso

59. Uma nota final para assinalar que não é explicado na exposição de motivos, nem resulta óbvio do teor do diploma aqui proposto, ou do objeto e âmbito de aplicação da Lei n.º 41/2004, a razão por que, no artigo 4.º da Proposta, se reconhece competência regulamentar ao membro do Governo responsável pela área da defesa quando é certo que a finalidade da transmissão dos dados aqui regulada é a da investigação criminal (cf. artigo 1.º da Proposta), mesmo considerando as funções desempenhadas hoje pela Polícia Judiciária Militar.

60. Especificamente quanto à regulamentação das condições de transmissão dos dados pessoais, devem estar definidos ainda no plano legislativo os parâmetros mínimos de orientação para o exercício da competência regulamentar, em especial, a vinculação de garantir a integridade e a confidencialidade dos dados pessoais objeto de transmissão.

61. E recorda que foi publicada a Portaria n.º 469/2009, de 28 de abril, na qual estão definidas com precisão as regras técnicas de transmissão da informação, de modo a garantir a confidencialidade e integridade dos dados transmitidos, bem como a auditabilidade de todos os acessos.

62. Recorda-se também que o sistema tecnológico previsto nessa portaria foi concebido e implementado tanto do lado do Ministério da Justiça como do lado das operadoras de comunicações eletrónicas. Todavia, primeiro pela Portaria n.º 131/2010, de 2 de março, e depois pela Portaria n.º 694/2010, de 16 de agosto, determinou-se o caráter facultativo da sua utilização por um período experimental, especificando-se ainda que este período cessaria quando tal fosse determinado por despacho conjunto dos membros do Governo, o que até à data não ocorreu.

63. A CNPD só pode, pois, recomendar a fixação de idêntico regime regulamentar e a determinação da sua efetiva aplicação.

III. Conclusão

64. Apesar de apenas prever o acesso para a finalidade de investigação criminal a dados pessoais relativos a comunicações eletrónicas conservados, pelas empresas que fornecem serviços de redes públicas e de comunicações eletrónicas, para efeitos de faturação e pagamento dos serviços de comunicações eletrónicas, a presente Proposta de Lei reduz substancialmente as garantias dos direitos fundamentais dos cidadãos, por comparação com o regime jurídico anterior de conservação e transmissão de dados pessoais relativos a comunicações eletrónicas (seja o que se encontrava previsto na Lei n.º 32/2008, de 17 de julho, sobre retenção dos dados relativos às comunicações eletrónicas, seja o que se encontra ainda previsto na Lei do Cibercrime).

65. Essa redução resulta da combinação de três disposições distintas: a previsão de acesso pelo Ministério Público aos dados pessoais relativos às comunicações eletrónicas sem controlo direto e prévio de um juiz; o alargamento da finalidade do acesso, agora para a investigação de, praticamente, quaisquer crimes independentemente da sua gravidade; e a imposição às operadoras que fornecem serviços de rede e de comunicações eletrónicas da conservação de mais dados pessoais de identificação e de tráfego do que os

necessários para a finalidade de faturação e pagamento dos serviços de comunicações eletrónicas com o titular dos dados.

66. Estas três previsões constituem, *per se*, uma restrição desproporcionada dos direitos fundamentais à reserva da vida privada, à autodeterminação informativa e ao livre desenvolvimento da personalidade, mas a sua previsão simultânea implica um estrangulamento das garantias fundamentais dos cidadãos no contexto da utilização de redes e comunicações eletrónicas, com os riscos de intrusão abusiva na vida privada dos cidadãos e de condicionamento das suas liberdades fundamentais.

67. Nessa medida, a Proposta de Lei contraria a jurisprudência nacional e europeia, em particular o teor do acórdão do Tribunal Constitucional n.º 262/2022, bem como a jurisprudência do Tribunal de Justiça da União Europeia e do Tribunal Europeu dos Direitos Humanos, representando uma restrição desproporcionada dos direitos fundamentais à reserva da vida privada, à autodeterminação informativa e ao livre desenvolvimento da personalidade, em violação do n.º 2 do artigo 18.º da Constituição da República Portuguesa e do n.º 1 do artigo 52.º da Carta dos Direitos Fundamentais da União Europeia.

68. Assim, com os fundamentos acima expostos, a CNPD recomenda:

i. A alteração dos artigos 2.º e 3.º da Proposta, no sentido de prever a necessidade de despacho autorizativo do juiz para o acesso aos dados pessoais relativos às comunicações eletrónicas;

ii. A eliminação da alínea *c)* do artigo 2.º da Proposta;

iii. A alteração do artigo 8.º da Proposta, eliminando os seguintes dados das alíneas *c) e d)* na nova redação dada por esse artigo ao n.º 2 do artigo 6.º da Lei n.º 41/2004: dados de tráfego relativos a *grupo data/hora da chamada*, *número de telefone* e os *dados associados ao início e fim do acesso* à Internet.

69. A CNPD recomenda ainda:

i. a clarificação do âmbito de aplicação da previsão de destruição dos dados, no artigo 5.º da Proposta;

ii. a reponderação, no artigo 4.º da Proposta, da opção de reconhecer competência regulamentar ao membro do Governo responsável pela área da defesa, no contexto do acesso aos dados *para fins de investigação criminal*;

iii. a imposição, no artigo 4.º da Proposta, de que a regulamentação assegure a confidencialidade e integridade dos dados pessoais objeto de transmissão, bem como a auditabilidade dessa transmissão em termos equivalentes aos estabelecidos na Portaria n.º 469/2009, de 28 de abril.

70. Finalmente, a CNPD assinala, a propósito do n.º 1 do artigo 3.º da Proposta, que, em conformidade com o direito à prestação de informações sobre o tratamento de dados, estendendo-se a notificação do acesso aos titulares dos dados transmitidos, tal implica a notificação não apenas às pessoas singulares objeto de investigação, mas também a todas as pessoas singulares com quem tenha havido comunicação ou tentativa de comunicação, o que aumenta significativamente o universo de titulares de dados a notificar.

Aprovado na reunião de 21 de junho de 2022

Filipa Calvão (Presidente)