PARECER/2021/74

I. Pedido

1. A Comissão dos Assuntos Constitucionais, Direitos, Liberdades e Garantias da Assembleia da República solicitou à Comissão Nacional de Proteção de Dados (CNPD) a emissão de parecer sobre a Proposta de Lei n.º 98/XIV/2.ª (Gov), que «Transpõe a Diretiva (UE) 2019/713, relativa ao combate à fraude e à contrafação de meios de pagamento que não em numerário».

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 (doravante, Lei de Execução) e, ainda, em resultado do disposto na alínea c), do n.º 1 do artigo 44.º da Lei n.º 59/2019, de 8 de agosto.

3. A CNPD já se pronunciou através do seu Parecer n.º 36/2021, de 23 de março, sobre o Projeto de Proposta de Lei n.º 678/XXII/2020 cujo conteúdo se mantém praticamente inalterado no diploma ora submetido. Assim, porque se mantêm pertinentes e necessárias as observações então produzidas, limita-se a reproduzir com pequenas adaptações o Parecer formulado.

II. Análise

4. A Proposta de Lei sob análise visa promover um conjunto de alterações a diversos diplomas em vigor. Em virtude da natureza dessas alterações, que se prendem com revisões das molduras penais aplicáveis, reformulações e aditamentos de tipos de crime, para além das necessárias e subsequentes compatibilizações em diplomas conexos[1], e uma vez que nelas não se encontram matérias relevantes de proteção de dados pessoais, a CNPD, salvo pontuais anotações de relevo, apenas fará incidir o seu parecer sobre os artigos 1.º, 4.º e 5.º.

[1] Falamos, aqui, das modificações de vários estatutos profissionais (administradores judiciais, advogados, solicitadores, notários, mediador de recuperação de empresas) e, bem assim, de regimes, como o do Estatuto das Instituições Particulares de Solidariedade Social; o dos documentos eletrónicos e da assinatura digital, do Regulamento da Caixa de Previdência dos Advogados e Solicitadores; do código das Associações Mutualistas e do Decreto-lei n.º 137/2019, de 13 de setembro, que aprova a nova estrutura organizacional da Polícia Judiciária.

5. Visa-se, com a presente de Proposta de Lei, promover alterações na legislação nacional que, de forma clara, a possam alinhar com um conjunto de obrigações de natureza penal impostas pela Diretiva (UE) 2019/713 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativa ao combate à fraude e à contrafação de meios de pagamento que não em numerário e que substitui a Decisão-Quadro 2001/413/JAI do Conselho (Diretiva (UE) 2019/713).

6. Não se trata, portanto, de uma transposição em sentido próprio de uma diretiva, mas apenas de um conjunto de específicas condições que a mesma prevê e que se entende não estarem devidamente acobertadas pela legislação portuguesa.

7. De entre estas sobressaem as relativas ao alargamento a pessoas coletivas da responsabilidade penal no quadro de ilícitos já hoje previstos no Código Penal[2].

8. Igualmente relevantes são as alterações propugnadas quanto à inserção, na previsão legal das normas incriminadoras existentes atualmente, dos "instrumentos de pagamento corpóreos que não em numerário contrafeitos e falsificados que não sejam cartões de crédito (por exemplo, cartões de débito)", cujas condutas são, ainda, concentradas na Lei n.º 109/2009, de 15 de setembro (Lei do Cibercrime).

9. Nesta senda, também se entende relevante apurar as molduras de algumas condutas já hoje punidas pela lei nacional[3] e, bem assim, nela aditar condutas descritas no artigo 5.º da Diretiva, a saber, "A detenção de um instrumento de pagamento não corpóreo que não em numerário obtido de forma ilícita, contrafeito ou falsificado para utilização fraudulenta, pelo menos se a origem ilícita for conhecida no momento da sua detenção;" e "A aquisição para si próprio ou para terceiro, incluindo a venda, a transferência ou distribuição, ou a disponibilização de um instrumento de pagamento não corpóreo que não em numerário obtido de forma ilícita, contrafeito ou falsificado para utilização fraudulenta.".

10. Aproveitando as alterações decorrentes da adequação da lei nacional às exigências da Diretiva, visa-se promover "uma nova inserção sistemática das normas, coadunando-se as disposições do Código Penal com as da Lei do Cibercrime" (cfr. exposição de motivos).

11. Além de tudo isto, "deixa-se claro que as incriminações nacionais abrangem igualmente atos praticados por referência a moedas virtuais (de que a *bitcoin* é vulgar exemplo), para além das outras moedas já reconhecidas pela nossa ordem jurídica como integrando um sistema de pagamentos: a moeda física, a moeda escritural e a moeda eletrónica.". A tal precisão junta-se a de "que os atos preparatórios dos crimes de falsidade informática

---

[2] Nos artigos 203.º a 205.º, 209.º a 211.º, 217.º, 218.º, 221.º, 223.º, 225.º, 231.º ou 232.º

[3] Nomeadamente o n.º 1 do artigo 6.º da Lei do Cibercrime).

e de contrafação de cartões ou outros dispositivos de pagamento são punidos independentemente da realização ou não das respetivas ações de falsificação e contrafação".

12. A par de todas estas alterações, promovem-se outras de menor alcance, como a do ajustamento do ponto de contacto previsto no artigo 21.º da Lei do Cibercrime (onde passa a figurar o Ministério Público, atenta a natureza da informação a trocar) e de vários diplomas[4] onde se torna consequentemente inevitável conjugar as novidades decorrentes da "transposição" com o teor dos primeiros. Neste nível, são ainda corrigidas remissões legais na Lei do Cibercrime (que passará a referir-se à Lei n.º 59/2019 e já não à revogada Lei n.º 67/98, de 26 de outubro) e "corrig[em-se] algumas expressões, desarmonias semânticas ou lapsos evidentes constantes do Código Penal".

13. Mais problemáticas são, porém, as novidades que se pretendem introduzir quer no artigo 17.º da Lei do Cibercrime, quer na Lei n.º 32/2008 (ainda que aqui se trate de uma operação de compatibilização das alterações da primeira com esta última).

i. Alterações ao artigo 17.º da Lei do Cibercrime

14. Atente-se na justificação apresentada na proposta para as alterações a promover ao artigo 17.º da Lei do Cibercrime:

"Noutro plano, e ainda que se trate de um aspeto não respeitante à transposição da Diretiva (UE) 2019/713, aproveita-se o ensejo para ajustar o artigo 17.º da Lei do Cibercrime, cujo teor tem gerado conflitos jurisprudenciais que prejudicam a economia processual e geram dúvidas desnecessárias.

Este ajustamento tem como propósito clarificar o modelo de apreensão de correio eletrónico e da respetiva validação judicial.

Visa-se, por um lado, esclarecer que a apreensão de mensagens de correio eletrónico ou de natureza similar está sujeita a um regime autónomo, que vigora em paralelo com o regime da apreensão de correspondência previsto no Código de Processo Penal. Este último regime apenas se aplica à apreensão de mensagens de correio eletrónico ou de natureza similar a título subsidiário, e com as necessárias adaptações.

[4] O Código de Processo Penal, o Decreto-Lei n.º 137/2019, de 13 de setembro, o Código das Associações Mutualistas, a Lei n.º 6/2018, de 22 de fevereiro, o Estatuto da Ordem dos Notários, o Estatuto da Ordem dos Solicitadores e dos Agentes de Execução, o Estatuto da Ordem dos Advogados, o Regulamento da Caixa de Previdência dos Advogados e Solicitadores, a Lei n.º 22/2013, de 26 de fevereiro, a Lei n.º 32/2008, de 17 de julho, a Lei n.º 52/2003, de 22 de agosto, à Lei n.º 5/2002, de 11 de janeiro, o Decreto-Lei n.º 290-D/99, de 2 de agosto, e o Estatuto das Instituições Particulares de Solidariedade Social.

Visa-se, por outro lado, esclarecer que a apreensão de mensagens de correio eletrónico ou de natureza similar guardadas num determinado dispositivo, embora incidindo sobre dados informáticos de conteúdo especial, não é tecnicamente diferente da apreensão de outro tipo de dados informáticos.

Assim, deve o Ministério Público, após análise do respetivo conteúdo, apresentar ao juiz as mensagens de correio eletrónico ou de natureza similar cuja apreensão tiver ordenado ou validado e que considere serem de grande interesse para a descoberta da verdade ou para a prova, ponderando o juiz a sua junção aos autos tendo em conta os interesses do caso concreto.

Esta solução procura replicar, no domínio das mensagens de correio eletrónico ou de natureza similar, a solução presentemente aplicável aos dados e documentos informáticos cujo conteúdo possa revelar dados pessoais ou íntimos, pondo em causa a privacidade do respetivo titular ou de terceiro, nos termos do n.º 3 do artigo 16.º da Lei do Cibercrime." (sublinhados nossos).

15. A proposta de redação do novo artigo 17.º que concretiza estas motivações traduziu-se no seguinte articulado:

> *"1- Quando, no decurso de uma pesquisa informática ou de outro acesso legítimo a um sistema informático, forem encontradas, armazenadas nesse sistema informático ou noutro a que seja permitido o acesso legítimo a partir do primeiro, mensagens de correio eletrónico ou de natureza semelhante que sejam necessárias à produção de prova, tendo em vista a descoberta da verdade, a autoridade judiciária competente autoriza ou ordena por despacho a sua apreensão.*
>
> *2- O órgão de polícia criminal pode efetuar as apreensões referidas no número anterior, sem prévia autorização da autoridade judiciária, no decurso de pesquisa informática legitimamente ordenada e executada nos termos do artigo 15.º, bem como quando haja urgência ou perigo na demora, devendo tal apreensão ser validada pela autoridade judiciária no prazo máximo de 72 horas.*
>
> *3- À apreensão de mensagens de correio eletrónico e de natureza semelhante aplica-se o disposto nos n.ºs 5 a 8 do artigo anterior.*
>
> *4- O Ministério Público apresenta ao juiz, sob pena de nulidade, as mensagens de correio eletrónico ou de natureza semelhante cuja apreensão tiver ordenado ou validado e que considere serem de grande interesse para a descoberta da verdade ou para a prova, ponderando o juiz a sua junção aos autos tendo em conta os interesses do caso concreto.*

5- Os suportes técnicos que contenham as mensagens apreendidas cuja junção não tenha sido determinada pelo juiz são guardados em envelope lacrado, à ordem do tribunal, e destruídos após o trânsito em julgado da decisão que puser termo ao processo.

6- No que se não encontrar previsto nos números anteriores, é aplicável, com as necessárias adaptações, o regime da apreensão de correspondência previsto no Código de Processo Penal."

16. Dispõe hoje o artigo 17.º da Lei do Cibercrime, sob a epígrafe "Apreensão de correio electrónico e registos de comunicações de natureza semelhante" o seguinte: "Quando, no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático, forem encontrados, armazenados nesse sistema informático ou noutro a que seja permitido o acesso legítimo a partir do primeiro, mensagens de correio electrónico ou registos de comunicações de natureza semelhante, o juiz pode autorizar ou ordenar, por despacho, a apreensão daqueles que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova, aplicando-se correspondentemente o regime da apreensão de correspondência previsto no Código de Processo Penal." (sublinhados nossos).

17. O regime da apreensão de correspondência previsto no Código de Processo Penal (CPP) é o que consta do artigo 179.º, onde se prevê que:

"(1) Sob pena de nulidade, o juiz pode autorizar ou ordenar, por despacho, a apreensão, mesmo nas estações de correios e de telecomunicações, de cartas, encomendas, valores, telegramas ou qualquer outra correspondência, quando tiver fundadas razões para crer que: a) A correspondência foi expedida pelo suspeito ou lhe é dirigida, mesmo que sob nome diverso ou através de pessoa diversa; b) Está em causa crime punível com pena de prisão superior, no seu máximo, a 3 anos; e c) A diligência se revelará de grande interesse para a descoberta da verdade ou para a prova.

(2) É proibida, sob pena de nulidade, a apreensão e qualquer outra forma de controlo da correspondência entre o arguido e o seu defensor, salvo se o juiz tiver fundadas razões para crer que aquela constitui objecto ou elemento de um crime.

(3) O juiz que tiver autorizado ou ordenado a diligência é a primeira pessoa a tomar conhecimento do conteúdo da correspondência apreendida. Se a considerar relevante para a prova, fá-la juntar ao processo; caso contrário, restitui-a a quem de direito, não podendo ela ser utilizada como meio de prova, e fica ligado por dever de segredo relativamente àquilo de que tiver tomado conhecimento e não tiver interesse para a prova." (sublinhado nosso).

18. Resulta, na perspetiva da CNPD, evidente, que o artigo 17.º da Lei do Cibercrime arquiteta um sistema de validação da apreensão de mensagens de correio eletrónico (ou registos de comunicações de natureza

semelhante) em (quase) tudo coincidente com o previsto no artigo 179.º do CPP[5]. Sendo o objeto da Lei do Cibercrime o *"estabelec[imento d]as disposições penais materiais e processuais, bem como as disposições relativas à cooperação internacional em matéria penal, relativas ao domínio do cibercrime e da recolha de prova em suporte electrónico"*, ela constitui, quanto aos elementos de prova em suporte eletrónico verdadeira *lex specialis* por contraponto ao CPP. Ainda assim, o legislador optou por concretizar a restrição do direito constitucional à inviolabilidade da correspondência, previsto no artigo 34.º da Constituição da República Portuguesa (CRP), com uma cláusula que praticamente replica o n.º 1 do artigo 179.º do CPP, salvo quando à tripla condição que neste inciso se aponta como condição para fundamentar a autorização ou ordem de apreensão.

19. Ora, se se aceita que uma alteração legislativa possa servir para superar *"conflitos jurisprudenciais que prejudicam a economia processual e geram dúvidas desnecessárias"*, já se apontam maiores dificuldades a admitir que essa modificação possa pretender superar esses problemas pela via da menorização de direitos fundamentais constitucionalmente consagrados – em particular, um direito fundamental que tem precisamente por objeto a reserva do conteúdo das comunicações.

20. Também se pode compreender *"que a apreensão de mensagens de correio eletrónico ou de natureza similar guardadas num determinado dispositivo, embora incidindo sobre dados informáticos de conteúdo especial, não é tecnicamente diferente da apreensão de outro tipo de dados informáticos"*, mas esta conclusão é incompreensível se se destinar a justificar a equiparação de dados pessoais e dados não pessoais. Com efeito, a CRP reserva não só uma esfera de proteção para a reserva da intimidade da vida privada, como melhor a concretiza no direito à inviolabilidade da correspondência, e ainda singulariza a proteção de dados pessoais neste catálogo de preceitos "diretamente aplicáveis".

21. Seria, por isso, injustificado, desde logo no plano constitucional, consagrar na legislação a indistinção entre dados pessoais e dados não pessoais. Ademais, tal constituiria uma latente violação do reconhecimento que é devido ao direito ao respeito pela vida privada e familiar como se encontra positivado no artigo 8.º da Convenção Europeia dos Direitos do Homem e, bem assim, pelos artigos 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia[6], respetivamente quanto ao respeito pela vida privada e familiar e à proteção de dados pessoais.

22. Temos, portanto, que um tal objetivo, declarado na exposição de motivos, contraria quer a Constituição, quer os compromissos internacionais do Estado português, sendo insondável a razão para a sua inclusão na Lei do Cibercrime.

---

[5] E artigo 178.º, quanto à correspondência aberta.

[6] A que acresce o artigo 52.º, pela sua relevância prática em matéria de restrições aos direitos fundamentais previstos na CDFUE.

23. E nem se diga, como é avançado na Proposta, que o que se pretende é a equiparação ao regime da apreensão de dados informáticos, constante do artigo 16.º, especificamente o previsto no n.º 3[7]. Desde logo, a apreensão de dados informáticos, ao contrário do correio eletrónico e dos registos de comunicações do artigo 17.º, não tem necessariamente que envolver dados pessoais ou reveladores da dimensão da vida privada dos visados, sendo essa a razão para que o sobredito n.º 3 do artigo 16.º acautele potenciais casos em que tal aconteça, reforçando-se as garantias dos cidadãos através da obrigatória intervenção do Juiz.

24. Depois, porque, ao contrário das comunicações, será habitual encontrar esta informação (*i.e.*, os dados informáticos) não vedada ou fechada (ou com indicação semelhante)[8], dependendo o conhecimento da existência de dados pessoais ou íntimos do contacto direto e inevitável com o conteúdo desses dados informáticos[9] ainda antes da potencial intervenção do Juiz.

25. Finalmente, por degradar o regime aplicável às comunicações, não deveria ser visto como o meio óbvio e idóneo para fazer face aos requisitos constitucionais que os n.ºs 2 e 3 do artigo 18.º da CRP colocam sempre que se pretenda limitar ou restringir os direitos, liberdades e garantias. Sobretudo quando tal degradação se aparta, em medida desproporcionada, do regime previsto no CPP para a apreensão de correspondência, o qual era, até agora, perfeitamente aplicável aos casos previstos no artigo 17.º da Lei do Cibercrime[10].

ii. A intervenção do Ministério Público à luz da jurisprudência do Tribunal de Justiça da União Europeia e a alteração à Lei n.º 32/2008

26. A alteração à Lei do Cibercrime decorrente da Proposta funda-se, como é assumido na exposição de motivos, na adaptação do ordenamento jurídico nacional ao previsto na Diretiva (UE) 2019/713. É facto que a referida lei se centra na disciplina penal e processual no domínio do cibercrime e da prova em suporte eletrónico, sendo sabido que "no estado atual do direito da União, cabe, em princípio, exclusivamente ao direito nacional determinar as regras relativas à admissibilidade e à apreciação, no âmbito de um processo penal instaurado contra pessoas suspeitas de atos de criminalidade, de informações e de elementos de prova"[11].

---

[7] *"Caso sejam apreendidos dados ou documentos informáticos cujo conteúdo seja susceptível de revelar dados pessoais ou íntimos, que possam pôr em causa a privacidade do respectivo titular ou de terceiro, sob pena de nulidade esses dados ou documentos são apresentados ao juiz, que ponderará a sua junção aos autos tendo em conta os interesses do caso concreto"*.

[8] A este ponto voltaremos com maior detalhe.

[9] Atente-se na definição que a alínea d) do artigo 2.º da Lei do Cibercrime oferece *"«Dados informáticos», qualquer representação de factos, informações ou conceitos sob uma forma susceptível de processamento num sistema informático, incluindo os programas aptos a fazerem um sistema informático executar uma função;"*

[10] Cfr. Acórdão do Tribunal da Relação de Lisboa de 6 de fevereiro de 2018, disponível em http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/a1b9fce5f23b342480258242004327a3?OpenDocument.

[11] Cfr. § 41 do acórdão do TJUE de 2 de março de 2021, no processo C-746/18.

27. Não deve, todavia, olvidar-se que o Direito da União Europeia vem crescendo em importância e relevância na conformação de legislação penal dos Estados-Membros[12]. De resto, a própria Lei do Cibercrime resulta da transposição para o direito nacional da Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro[13], a que acresce o facto de adaptar o direito interno à Convenção sobre Cibercrime do Conselho da Europa. E o ensejo do legislador em, pela primeira vez, operar alterações à Lei n.º 32/2008, de 7 de julho, não pode deixar de convocar uma reflexão séria sobre a sua adequação global em face do ordenamento jurídico da União.

28. É inegável que a projeção do direito da União e da Convenção Europeia dos Direitos do Homem no direito interno tem de ser aqui considerada. E, bem assim, devem ser ponderadas as ponderações dos Tribunais competentes[14] para julgar, a final, da conformidade do direito interno com as disposições da União e com a Convenção.

29. Em matéria de prova digital, ganha particular relevância o percurso interpretativo que o TJUE tem protagonizado nos últimos anos, em especial na avaliação da Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006, e também das leis nacionais que a transpuseram.

30. Dispensamo-nos de descrever com detalhe todos os acórdãos que sobre ela se têm vindo a debruçar, sendo suficiente referir que a Diretiva foi considerada inválida em 2014, no acórdão *Digital Rights Ireland, Ltd.*, de 8 de abril de 2014, no âmbito de reenvios prejudiciais que deram origem aos processos C-293/12 e C-594/12[15].

31. A CNPD emitiu a Deliberação 641/2017[16], onde, como consequência da declaração de invalidade resultante do acórdão do TJUE, "[e]ntende[u] (...) ser seu dever alertar a Assembleia da República para a necessidade de reavaliar a Lei n.º 32/2008, de 17 de julho, em termos de conformidade com a Carta, mas também com a CRP, já que os direitos fundamentais restringidos por aquele regime têm consagração constitucional e a restrição legal de tais direitos obedece nos termos constitucionais ao mesmo princípio da proporcionalidade.". Tendo concluído, entre outras, que "a Lei n.º 32/2008 contém normas que preveem a restrição ou ingerência nos direitos fundamentais ao respeito pela vida privada e pelas comunicações e à proteção dos dados pessoais (artigos 7.º

---

[12] Atente-se no artigo de Anabela Miranda Rodrigues, *O Direito Penal europeu à luz do princípio da necessidade – o caso do abuso de mercado*, publicado na Católica Law Review, Vol. 1, n.º 3, nov. 2017, disponível em https://fd.lisboa.ucp.pt/asset/3041/file.

[13] Entretanto revogada pela Diretiva 2013/40/UE do Parlamento Europeu e do Conselho, de 12 de agosto de 2013, relativa a ataques contra os sistemas de informação.

[14] Respetivamente o Tribunal de Justiça da União Europeia e do Tribunal Europeu dos Direitos do Homem.

[15] Disponível em http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d63d34ffbab785491ab755b34740570fe7.e34KaxiLc3eQc40LaxqMbN4Pax0Qe0?text=&docid=150642&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=48371.

[16] Disponível em https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/101085.

e 8.º da Carta dos Direitos Fundamentais da União Europeia) com grande amplitude e intensidade, em clara violação do princípio da proporcionalidade e, portanto, em violação do n.º 1 do artigo 52.º da Carta.

32. Com os mesmos fundamentos, verifica-se uma restrição desproporcionada dos direitos à reserva da intimidade da vida privada, à inviolabilidade das comunicações e à proteção de dados pessoais, em violação do disposto no n.º 2 do artigo 18.º da Constituição da República Portuguesa."[17]

33. O presente parecer não se destina a recalcar os argumentos aí expostos para justificar a pertinente necessidade de reavaliar a Lei n.º 32/2008, de 7 de julho, à luz da jurisprudência do TJUE, o que ainda não aconteceu, remetendo-se, neste particular, para a referida deliberação, cujo conteúdo mantém total atualidade. Aliás, encontra-se em apreciação no Tribunal Constitucional um pedido de fiscalização de constitucionalidade do referido diploma, submetido pela Provedora de Justiça.

34. Considera-se, no entanto, imprescindível reforçar a sugestão de revisão dessa lei à luz da evolução da jurisprudência recente do TJUE, a qual só veio confirmar as conclusões constantes da deliberação da CNPD e introduzir novos elementos de análise aos quais o legislador nacional não pode deixar de conferir significativa importância.

35. Sem prejuízo das úteis clarificações introduzidas pelo Acórdão do TJUE de 6 de outubro de 2020, no processo C-623/17, sobretudo no que respeita à delimitação das exceções ou restrições permitidas pelo n.º 1 do artigo 15.º da Diretiva 2002/58[18], julgamos ser prioritário apontar aqui as conclusões do Acórdão do TJUE, de 2 de março, no processo C-746/18, porquanto aqui se deteve o tribunal sobre a legitimidade do Ministério Público autorizar o acesso de uma autoridade pública aos dados de tráfego e aos dados de localização para fins de instrução penal.

36. Colocavam-se neste caso três questões ao TJUE, sendo que, para o presente parecer, nos deteremos apenas na terceira, pela especial relevância que demonstra.

---

[17] Cfr. conclusões da deliberação citada.

[18] Que assim dispõe: *"Os Estados-Membros podem adoptar medidas legislativas para restringir o âmbito dos direitos e obrigações previstos nos artigos 5.º e 6.º, nos n.os 1 a 4 do artigo 8.º e no artigo 9.º da presente directiva sempre que essas restrições constituam uma medida necessária, adequada e proporcionada numa sociedade democrática para salvaguardar a segurança nacional (ou seja, a segurança do Estado), a defesa, a segurança pública, e a prevenção, a investigação, a detecção e a repressão de infracções penais ou a utilização não autorizada do sistema de comunicações electrónicas, tal como referido no n.º 1 do artigo 13.º da Directiva 95/46/CE. Para o efeito, os Estados-Membros podem designadamente adoptar medidas legislativas prevendo que os dados sejam conservados durante um período limitado, pelas razões enunciadas no presente número. Todas as medidas referidas no presente número deverão ser conformes com os princípios gerais do direito comunitário, incluindo os mencionados nos n.os 1 e 2 do artigo 6.º do Tratado da União Europeia."*.

37. Tal como a postulou o tribunal, a questão prejudicial assim se resumia *"se o artigo 15.°, n.° 1, da Diretiva 2002/58, lido à luz dos artigos 7.°, 8.°, 11.° e 52.°, n.° 1, da Carta, deve ser interpretado no sentido de que se opõe a uma regulamentação nacional que atribui competência ao Ministério Público, cuja missão é dirigir a instrução penal e exercer, sendo caso disso, a ação pública num processo posterior, para autorizar o acesso de uma autoridade pública aos dados de tráfego e aos dados de localização para fins de instrução penal."*[19]

38. Partindo da ideia incontroversa de que *"é verdade que cabe ao direito nacional determinar as condições em que os prestadores de serviços de comunicações eletrónicas devem conceder às autoridades nacionais competentes o acesso aos dados de que dispõem [o TUE ressalva que], para satisfazer a exigência de proporcionalidade, tal regulamentação deve prever regras claras e precisas que regulem o alcance e a aplicação da medida em causa e imponham exigências mínimas, de modo que as pessoas cujos dados foram conservados disponham de garantias suficientes que permitam proteger eficazmente esses dados pessoais contra os riscos de abuso."*[20]

39. Essas regras "materiais e processuais" devem *"basear-se em critérios objetivos para definir as circunstâncias e as condições em que o acesso aos dados em causa deve ser concedido às autoridades nacionais competentes."*[21]. Sendo que *"é essencial que o acesso das autoridades nacionais competentes aos dados conservados esteja, em princípio, sujeito a uma fiscalização prévia efetuada por um órgão jurisdicional ou por uma entidade administrativa independente e que a decisão desse órgão jurisdicional ou dessa entidade seja tomada na sequência de um pedido fundamentado dessas autoridades apresentado, nomeadamente, no âmbito de processos de prevenção, de deteção ou de perseguição penal. Em caso de urgência devidamente justificada, a fiscalização deve ser efetuada em prazos curtos"*[22]

40. E, prosseguindo, nota, *"Essa fiscalização prévia exige (...) que o órgão jurisdicional ou a entidade encarregada de efetuar a referida fiscalização prévia disponha de todas as atribuições e apresente todas as garantias necessárias com vista a assegurar uma conciliação dos diferentes interesses e direitos em causa. Quanto, mais especificamente, a um inquérito penal, tal fiscalização exige que esse órgão jurisdicional ou essa entidade possa assegurar um justo equilíbrio entre, por um lado, os interesses ligados às necessidades do inquérito no âmbito da*

---

[19] Cfr. § 46 do acórdão.
[2020] Cfr. § 48 do acórdão.
[21] Cfr. § 49 e 50 do acórdão.
[22] Cfr. § 51 do acórdão.

luta contra a criminalidade e, por outro, os direitos fundamentais ao respeito da vida privada e à proteção dos dados pessoais das pessoas às quais o acesso diz respeito."[23]

Donde, "...a exigência de independência que a autoridade encarregada de exercer a fiscalização prévia (...) deve satisfazer impõe que essa autoridade tenha a qualidade de terceiro em relação à autoridade que pede o acesso aos dados, de modo que a primeira esteja em condições de exercer essa fiscalização de maneira objetiva e imparcial, ao abrigo de qualquer influência externa. Em especial, no domínio penal, a exigência de independência implica (...) que a autoridade encarregada dessa fiscalização prévia, por um lado, não esteja envolvida na condução do inquérito penal em causa e, por outro, tenha uma posição de neutralidade relativamente às partes no processo penal.

Não é esse o caso de um Ministério Público que dirige o inquérito e exerce, sendo caso disso, a ação pública. Com efeito, o Ministério Público tem por missão, não decidir com total independência um litígio mas submetê-lo, se necessário, ao órgão jurisdicional competente, enquanto parte no processo que exerce a ação penal.

A circunstância de o Ministério Público ser obrigado, em conformidade com as regras que regulam as suas competências e o seu estatuto, a verificar os elementos incriminatórios e ilibatórios, a garantir a legalidade da instrução do processo e a agir unicamente nos termos da lei e segundo a sua convicção não basta para lhe conferir o estatuto de terceiro em relação aos interesses em causa na aceção descrita no n.° 52 do presente acórdão.

Daqui resulta que o Ministério Público não está em condições de efetuar a fiscalização prévia referida no n.° 51 do presente acórdão."[24]

41. Ora, o TJUE é inequívoco na imprescindibilidade de mediação por um juiz ou autoridade independente no acesso a dados conservados ao abrigo da Diretiva 2002/58/CE[25]. Este é mais um critério que se junta aos já definidos por este Tribunal[26] e que se aplica diretamente ao contexto nacional, uma vez que também aqui, "[o] Ministério Público representa o Estado, defende os interesses que a lei determinar, participa na execução da política criminal definida pelos órgãos de soberania, exerce a ação penal orientado pelo princípio da legalidade e defende a legalidade democrática, nos termos da Constituição, do presente Estatuto e da Lei"[27], "goza[ndo apenas] de autonomia em relação aos demais órgãos do poder central, regional e local"[28].

---

[23] Cfr. § 52 do acórdão.
[24] Cfr. §§ 54 a 57 do acórdão.
[25] Conservação que, em Portugal, se encontra disciplinada na Lei n.º 32/2008, de 7 de julho.
[26] Cfr. ponto 2 das conclusões da CNPD na Deliberação citada.
[27] Cfr. artigo 2.º da Lei n.º 68/2019, de 27 de agosto (Estatuto do Ministério Público/EMP).
[28] Cfr. n.º 1 do artigo 3.º do EMP.

42. Significa isto, no contexto do presente parecer, que, em primeiro lugar, deveria o legislador aproveitar a oportunidade com que se depara de alterar a Lei n.º 32/2008, de 7 de julho, detendo-se na revisão detalhada dos critérios substantivos e processuais que nela vigoram para legitimar a conservação e o acesso aos dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações. Ao invés de se limitar, como se assiste na proposta de lei, a aditar uma conduta ao catálogo das já existentes no conceito de "crimes graves", previsto na alínea *g)* do artigo 1.º da também chamada Lei da Retenção de Dados, o legislador poderia e deveria ter expandido o ímpeto de revisão por forma a superar o atual contexto de insustentável fragilidade em que o diploma se encontra.

43. A relação desta incursão pela jurisprudência do TJUE com as alterações propostas à Lei do Cibercrime, não dizem respeito à obrigação de o legislador nacional aplicar, *ipsis verbis*, à revisão desta lei o que se defende para a Lei da Retenção de Dados. De todo o modo, não pode deixar de se retirar consequências deste acórdão para outros diplomas legislativos que prevejam soluções, como a agora proposta para o artigo 17.º, de permitir ao Ministério Público uma ampla margem de atuação na validação e ordem de apreensão das mensagens de correio eletrónico ou de natureza semelhante. Ora, sem postergar a competência dos Estados-Membros para definir o regime penal e processual penal interno, a conjugação dos ordenamentos jurídicos nacionais com o que provêm da União Europeia – sobretudo quando parcial ou totalmente ligados por obrigações de transposição de diretivas –, deve, pelo menos, considerar as implicações estruturais que decorrem das obrigações dos Estados-Membros, aqui, concretamente, quanto ao respeito pelo disposto na Carta dos Direitos Fundamentais da União.

44. No fundo, a perplexidade surge perante a pretensão de se admitir uma ingerência deste nível relativamente a dados incontroversamente sensíveis, como o são os das comunicações, quando o TJUE exige critérios bem mais rígidos para admitir o acesso a outros dados pessoais (como os de tráfego e localização)[29]. E é reforçada pela manifesta contradição com o disposto no n.º 1 do artigo 52.º da Carta dos Direitos Fundamentais da União Europeia.

45. Também no plano da jurisprudência do TEDH, se é verdade que não se pode proceder a uma aplicação direta à presente Proposta dos julgamentos que respeitavam à avaliação do acesso a dados das comunicações por

[29] Pese embora a posição da CNPD convirja totalmente com a do TJUE, como se nota no Ponto II da Deliberação citada: "*Com efeito, são dados que revelam a todo o momento aspetos da vida privada e familiar dos indivíduos: permitindo rastrear a localização do cidadão ao longo do dia, todos os dias (desde que transporte o telemóvel ou outro dispositivo eletrónico de acesso à Internet) com quem contacta (chamada – inclusive as tentadas e não concretizadas – por telefone ou telemóvel, envio ou receção de SMS, MMS, ou de correio eletrónico), duração e regularidade dessas comunicações e que sítios da Internet consulta.*"

parte dos serviços secretos ou de informações[30], mantém-se a perplexidade perante a alteração projetada do artigo 17.º face ao disposto no artigo 8.º da Convenção Europeia dos Direitos do Homem.

III. Conclusão

46. Com os fundamentos acima expostos, entende a CNPD que:

a. As alterações ao artigo 17.º da Lei do Cibercrime, tal como se encontram na Proposta de Lei em análise, representam uma manifesta degradação do nível de proteção dos cidadãos num domínio crítico da sua esfera privada, como é o das comunicações;
b. Ao divergir incontroversamente do regime previsto no artigo 179.º do CPP, a Proposta de Lei introduz restrições adicionais e não fundamentadas aos direitos, liberdades e garantias à inviolabilidade das comunicações e, reflexamente, à proteção de dados pessoais, como vêm consagrados nos artigos 34.º e 35.º da CRP, respetivamente;
c. Admitir que o Ministério Público possa, sem prévio controlo do Juiz de Instrução Criminal, ordenar ou validar a apreensão de comunicações eletrónicas ou de registos similares desprotege excessivamente as pessoas eventualmente suspeitas ou que tenham incidentalmente interagido com esses suspeitos, sendo que a exigência de intervenção do Juiz de Instrução, nos mesmos termos do artigo 179.º do CPP, nunca pode ser vista como desvirtuadora do princípio acusatório que preside ao processo penal em Portugal;
d. De resto, e atento o teor do recente acórdão do TJUE, de 2 de março, no processo C-746/18, onde se afasta a possibilidade de uma entidade em tudo semelhante – nos poderes e na dependência hierárquica – ao Ministério Público português poder aceder aos dados de tráfego e de localização, no quadro de um processo penal e em concretização das exceções previstas no n.º 1 do artigo 15.º da Diretiva 2002/58/CE, sem prévia autorização de um Juiz ou entidade independente, só pode ter-se por inadmissível a alteração proposta para o artigo 17.º da Lei do Cibercrime, por manifesta contradição com o disposto no artigo 52.º da Carta dos Direitos Fundamentais da UE (e sem prescindir do disposto no n.º 2 do artigo 18.º da CRP).

---

[30] Cfr. Acórdão *Big Brother Watch and others v. the United Kingdom*, de 13 de setembro de 2018 (disponível em http://hudoc.echr.coe.int/fre?i=001-140713) e Acórdão *Roman Zakharov v. Russia*, de 4 de dezembro de 2015 (disponível em http://hudoc.exec.coe.int/fre?i=004-14134).

47. Quanto à alteração à Lei n.º 32/2008, de 7 de julho (Lei da Retenção de Dados), que vem proposta no artigo 4.º da Proposta, limitando-se a aditar uma nova conduta às já constantes do conceito de "crime grave", mal se compreende que, depois de o TJUE ter declarado inválida a Diretiva que esta lei transpõe e quando está a ser julgada a sua própria constitucionalidade, a alteração legislativa tenha este teor, em vez de corrigir ou suprir as normas em crise. Entende a CNPD, por isso, que ao legislador só resta proceder à revisão profunda e meticulosa do regime substantivo e processual da referida lei. Tal afirma-se como um imperativo resultante da jurisprudência constante do TJUE e condição essencial para superar a atual situação de fragilidade, para dizer o menos, em que a lei se encontra.

Lisboa, 8 de junho de 2021

Maria Cândida Guedes de Oliveira (Relatora)