

PARECER/2021/152

I. Pedido

1. A Ministra da Modernização do Estado e da Administração Pública solicitou à Comissão Nacional de Proteção de Dados (CNPDP) a emissão de parecer sobre o Projeto de Portaria relativo à «Segunda alteração À Portaria n.º 77/2018, de 16 de março, que procede à regulamentação necessária ao desenvolvimento da Chave Móvel Digital (CMD)».
2. O pedido de parecer vem instruído com a avaliação de impacto sobre a proteção de dados (AIPD).
3. A CNPDP 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, alínea b) do n.º 3 do artigo 58.º e 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 da Lei n.º 58/2019, de 8 de agosto, que executa na ordem jurídica interna o RGPD.

II. Análise

4. O presente Projeto de Portaria procede à alteração da Portaria n.º 77/2018, de 16 de março, concretizando as alterações introduzidas pelo Decreto-Lei n.º 88/2021, de 3 de novembro, na Lei n.º 37/2014, de 26 de junho.
5. A CNPDP constata que as disposições do Projeto de Portaria, com pontuais exceções, reproduzem ou suportam-se em normas constantes daquele Decreto-Lei, sem que as incongruências e a maior parte das omissões do mesmo tenham sido corrigidas ou integradas, não obstante a CNPDP para elas ter chamado a atenção no Parecer/2021/99¹, de 22 de julho, que emitiu sobre o projeto daquele diploma legal. Nessa medida, a CNPDP reiterará aqui parte das observações e recomendações que deixou vertidas no referido parecer. Vejamos.

i. A insuficiência da regulamentação do tratamento de dados biométricos através da tecnologia de reconhecimento facial

6. Desde logo, assinala-se que elementos essenciais do tratamento de dados pessoais biométricos, que a CNPDP, no seu parecer, recomendava serem fixados no diploma legal, não só neste não ficaram vertidos, como também não se encontram determinados no Projeto de Portaria.

¹ Disponível em <https://www.cnpdp.pt/umbraco/surface/cnpdpDecision/download/121905>

7. Com efeito, sobre os tratamentos de dados pessoais decorrentes da utilização da tecnologia de reconhecimento facial no pedido para obtenção da CMD, vertido no artigo 2.º da Lei n.º 37/2014, na sua versão atual, continuam por densificar os elementos e condições da sua realização e por definir garantias dos direitos dos titulares dos dados.

8. Na realidade, os artigos 4.º-A e 4.º-B agora aditados pelo Projeto de Portaria não definem, desde logo, quem é o responsável pelo tratamento de dados pessoais. Note-se que a indicação, que consta do n.º 8 do artigo 2.º da Lei n.º 37/2014, de que a AMA, IP., *é a responsável pela gestão e segurança da infraestrutura tecnológica que suporta a CMD, nomeadamente o sistema de geração e envio dos códigos numéricos de utilização única e temporária*, não é elucidativa quanto a quem é o responsável pelo tratamento de dados, nos termos enunciados na alínea 7) do artigo 4.º do RGPD².

9. Ademais, o Projeto de Portaria, tal como o diploma legal que vem regulamentar, não define os dados pessoais objeto de tratamento e, especificamente, não explicita quais as *imagens do rosto recolhidas eletronicamente em tempo real* (cf. alínea e) do n.º 6 e ainda n.ºs 17 e 18 do artigo 2.º da Lei n.º 37/2014): se a imagem visualizada em tempo real no dispositivo móvel do cidadão, se uma fotografia (*selfie*) tirada no momento e enviada pelo cidadão, se aí se incluem também as minúcias biométricas e se eventualmente a imagem do rosto que consta do cartão de cidadão. Não se compreendendo por que razão se considera desnecessária a especificação dos dados pessoais objeto de tratamento, quando esse é um elemento essencial do tratamento, especialmente quando em causa esteja o tratamento de dados biométricos.

10. Acresce que não há, no Projeto de Portaria, qualquer explicação do processo de tratamento dos dados pessoais, para além da referência à comparação das *imagens do rosto recolhidas eletronicamente em tempo real* com a imagem facial constante do sistema de informação responsável pelo ciclo de vida do cartão de cidadão, *de forma automatizada, com recurso a software de deteção de vida* (previsto no n.º 17 do artigo 2.º da Lei n.º 34/2017), limitando-se o Projeto de Portaria, no n.º 2 do artigo 4.º-A agora introduzido na Portaria n.º 77/2018, a afirmar que «[o] registo [...] é realizado em conformidade com os procedimentos estabelecidos pelo Gabinete Nacional de Segurança sobre identificação de pessoas físicas através de procedimentos de identificação à distância com recurso a sistemas biométricos automáticos de reconhecimento facial».

11. Ora assim, nem o diploma legal, como se impunha, nem as portarias que o regulamentam oferecem o mínimo de previsibilidade para os cidadãos quanto aos tratamentos de dados pessoais a realizar pela Administração Pública, entre os quais constam o responsável pelo tratamento, os dados objeto de tratamento

² Uma vez que a responsabilidade pela gestão e segurança de uma infraestrutura tecnológica não é equiparável à responsabilidade pelo tratamento de dados pessoais que no contexto da mesma se realize.

e os prazos de conservação. Se tal vem indicado, no n.º 3 do artigo 6.º do RGPD, para a generalidade dos tratamentos de dados pessoais, mais premente se torna quando em causa estão dados pessoais que integram as categorias especiais definidas no n.º 1 do artigo 9.º do RGPD, como é precisamente o caso dos *dados biométricos para identificar uma pessoa de forma inequívoca*.

12. No Projeto de Portaria, tal como, aliás, terá sucedido no plano legislativo, parece presumir-se que, como o fundamento de licitude do tratamento de dados biométricos é o consentimento do titular dos dados (cf. n.ºs 17 e 19 do artigo 2.º da Lei n.º 37/2014), é dispensável a identificação nos respetivos diplomas legal e regulamentar dos elementos imprescindíveis à perceção de que dados pessoais são tratados e quais as consequências ou riscos, quando, na verdade, o consentimento para ser juridicamente relevante tem de ser *informado*.

13. Estando em causa, como pressupõe o sistema de reconhecimento facial, uma tecnologia de Inteligência Artificial de autoaprendizagem, que, portanto, analisa com autonomia, através de sistema de rede neuronal profunda (*Deep Learning*), os dados biométricos do rosto de cada cidadão, a explicação do que faz esse sistema é essencial – como se processam os dados biométricos «de forma automatizada» (v.g., que imagens são analisadas, o *rationale* ou a lógica subjacente ao tratamento, as consequências e riscos para o titular dos dados, etc.) para que um qualquer cidadão possa, em liberdade, optar pela sua utilização e consentir nas operações a realizar. Só que o Projeto nada diz sobre a tecnologia para deteção de vida e, no entanto, na AIPD afirma-se a utilização de algoritmos de *Deep Learning* para verificação da veracidade do cartão de cidadão.

14. Ainda que recaia sobre o responsável pelo tratamento o dever de prestar a informação, como impõe a alínea f) do n.º 2 do artigo 13.º do RGPD, a verdade é que um diploma que tem por objeto regulamentar este específico tratamento de dados pessoais tem que assumir o grau de previsibilidade e de densificação exigível num Estado de Direito e, portanto, conter elementos que permitam aos cidadãos fazer uma opção informada e consciente.

15. Até porque se corre o risco de, em concreto, se pretender que tal informação decorre já da lei e da portaria e nessa medida ficar aquele dispensado do cumprimento do dever (cf. o n.º 4 do artigo 13.º do RGPD, que admite essa dispensa quando e na medida em que o titular dos dados já tiver conhecimento das informações), quando na verdade os elementos do tratamento que a lei e o Projeto de Portaria revelam são escassos para a plena compreensão do mesmo e das suas implicações.

16. Entende, por isso, a CNPD que deve definir-se, com mais detalhe no texto do Projeto de portaria, os principais elementos e o processo (a lógica, se se preferir) do tratamento automatizado dos dados biométricos no âmbito da tecnologia utilizada para o reconhecimento facial e para verificação de outros dados pessoais,

insistindo que um consentimento *não informado* não é suficiente para legitimar os tratamentos de dados especiais ou sensíveis que aqui são objeto de previsão.

ii. A subcontratação e a reutilização dos dados biométricos para outra finalidade

17. Importa ainda insistir na previsão da reutilização da *imagem da frente e do verso do cartão de cidadão* para uma finalidade distinta, o *desenvolvimento evolutivo da CMD*, prevista no n.º 19 do artigo 2.º da Lei n.º 37/2014.

18. Tendo a CNPD chamado a atenção no seu Parecer sobre o Projeto de decreto-lei que esta previsão carecia de densificação normativa, a qual ocorreu apenas parcialmente na versão aprovada do Decreto-lei n.º 88/2021, muito se estranha que o Projeto de Portaria seja quanto a este novo tratamento de dados pessoais totalmente omissos.

19. A única exigência de segurança dos dados pessoais que o preceito legal em causa prevê é a cifragem da imagem do cartão de cidadão³. Mas a cifragem dos dados pessoais pelo responsável pelo tratamento, ou por um seu subcontratante, não acautela a utilização por qualquer um deles para finalidades diferentes.

20. Especificamente a este propósito, mas com considerações que são pertinentes para todo o tratamento dos dados biométricos, a CNPD insiste na necessidade de o Projeto de Portaria enquadrar o regime de subcontratação no âmbito do tratamento de dados biométricos e outros dados pessoais com recurso a tecnologia de *Deep Learning* para reconhecimento facial e para verificação do cartão de cidadão.

21. A questão é tanto mais importante quando em causa está a disponibilização voluntária, pelos cidadãos, a uma entidade administrativa dos respetivos dados biométricos para efeito último de utilização de mecanismos de autenticação e de assinatura digital qualificada, vontade que é formada no pressuposto – não expressamente afastado pela lei que prevê o tratamento – de que é a entidade administrativa quem recolhe, analisa e conserva tais dados.

22. A hipótese de a entidade pública responsável pelo tratamento subcontratar um terceiro para realizar, de facto, o referido tratamento suscita novas questões na perspetiva da proteção de dados, que poderão não ser irrelevantes também na tomada da decisão por parte do cidadão. Entre tais questões apresenta-se, em primeira linha, a de saber quem assegura o armazenamento dos dados biométricos.

³ Reitera-se que a afirmação no n.º 19.º do artigo 2.º da Lei n.º 34/2017 de que os *dados armazenados [...] não ficam associados ao cidadão* suscita a maior perplexidade, pois que mesmo que esteja apenas em causa a imagem do rosto do cidadão, a desassociação do cidadão de pouco serve neste contexto. Precisamente, os dados biométricos são suficientes para identificar o cidadão, por permitir estabelecer uma relação unívoca com o cidadão, razão por que esta pseudonimização aqui anunciada não mitiga substancialmente os riscos que uma base de dados desta natureza sempre implica.

23. Na verdade, mesmo na hipótese de essa base de dados biométricos estar situada em território de um Estado-Membro da União, é essencial garantir que a empresa subcontratante e a subsubcontratante não se encontram sujeitas a regras jurídicas vinculativas de um Estado terceiro que possam afetar a proteção garantida no território onde está alojada a base de dados.

24. É precisamente o que sucede neste caso, de acordo com o declarado na AIPD (cf. 5.1.17): a empresa onde está alojada a plataforma que realiza as validações associadas aos procedimentos de identificação à distância é a AWS (*Amazon Web Services, Inc*), com sede nos Estados Unidos da América, que é um Estado terceiro que apresenta regras jurídicas que vinculam esta empresa a disponibilizar a determinadas autoridades públicas desse Estado os dados por si conservados ou tratados, como resulta da jurisprudência do Tribunal de Justiça da União Europeia – cf. acórdão *Schrems II*, de 16.07.2020 (C-311/18).

25. Ora, esta situação, tendo em conta a jurisprudência europeia citada, salvo demonstração da adoção de medidas suplementares de proteção, não se afigura admissível face aos artigos 44.º e 46.º do RGPD, em especial tendo em conta a natureza sensível da informação que, insiste-se, ainda que pudesse ser cifrada – e não pode porquanto impedir a prossecução da finalidade –, sempre permite a identificação dos titulares dos dados. E não se encontra, na AIPD apresentada, qualquer avaliação de risco especificamente sobre este tratamento de dados pessoais, em contradição com o n.º 1 do artigo 46.º do RGPD.

26. Reitera-se que o consentimento para ser juridicamente relevante e, portanto, poder legitimar uma operação que implica ou é suscetível de implicar o fluxo internacional de dados pessoais sensíveis para um Estado terceiro sem proteção adequada tem de preencher os atributos da alínea 11) do artigo 4.º do RGPD, o que, nos termos da Lei n.º 37/2014 e do Projeto de Portaria, não está assegurado, face à omissão de todos os aspetos relativos às relações de subcontratação e subsubcontratação.

27. Assim, a CNPD recomenda que no Projeto de Portaria se acautele o risco de transferência de dados biométricos para Estados terceiros que não garantam proteção adequada, em conformidade com a jurisprudência do Tribunal de Justiça da União Europeia.

iii. Alterações introduzidas pelo artigo 2.º do Projeto de Portaria

28. Finalmente, importa assinalar um aspeto do regime jurídico constante da Portaria e do Projeto de Portaria relativo aos dados pessoais tratados para efeito do registo. Nos termos do artigo 2.º da Portaria n.º 77/2018, na nova versão agora projetada, o registo implica a associação do número de identificação civil, número de identificação fiscal ou número de passaporte, acrescentando-se que pode também ser associado o endereço eletrónico.

29. Ora, a CNPD apenas questiona o disposto na parte final do n.º 1 do artigo 2.º porque a previsão de que não tem de ser associado o endereço torna ou pode tornar inexecutável o disposto no n.º 3 do artigo 7.º do Projeto. Com efeito, salvo se for indicado outro meio alternativo de comunicação, não é possível alterar o número do telemóvel em caso de perda de acesso ao número registado.

30. Aliás, na AIPD (cf. 6.1.3.2) é indicado que a adesão à CMD é terminada caso o titular não insira o endereço de correio eletrónico; contudo, o Projeto de Portaria identifica este dado como opcional ao referir «podendo também associar-se o endereço de correio eletrónico».

31. Nessa medida, recomenda-se a ponderação do carácter opcional do fornecimento do endereço eletrónico, na parte final do n.º 1 do artigo 2.º, ou a explicitação no n.º 3 do artigo 7.º de que a possibilidade de alteração do número de telemóvel depende do fornecimento prévio, por parte do titular dos dados, de um contacto alternativo. E, sobretudo, que essa informação seja disponibilizada no sítio da Internet, para que o cidadão possa tomar a decisão em plena liberdade quanto a fornecer ou não esse dado pessoal.

32. Finalmente, quanto ao n.º 6 do artigo 6.º não se alcança o que seja o «atendimento telefónico mediado», que não tem previsão legal, e que traduz um novo meio de tratamento de dados pessoais. Nem parece ter sido avaliado o risco específico colocado por via da utilização desse meio, uma vez que na AIPD é referido o *funcionário do registo (mediador)* apenas para as situações de videoconferência.

III. Conclusão

33. A CNPD entende que o presente Projeto de Portaria padece de omissões que já se tinham assinalado no projeto de diploma legal que alterou a Lei n.º 37/2014, em especial porque, estando em causa o tratamento de dados biométricos com recurso a tecnologias de Inteligência Artificial de redes neuronais profundas, não define com detalhe os principais elementos do tratamento, bem como o processo (a lógica) do tratamento automatizado dos dados biométricos no âmbito da tecnologia utilizada, de modo que o cidadão possa estar suficientemente informado para poder optar pela sua utilização e dar um consentimento informado e livre.

34. Assim, e com os fundamentos desenvolvidos supra, a CNPD recomenda a previsão dos principais elementos dos tratamentos com tecnologia de *Deep Learning* para reconhecimento facial, da tecnologia para deteção de vida, da tecnologia de *Deep Learning* para verificação da veracidade do cartão de cidadão (v.g., o responsável pelo tratamento, os dados pessoais objeto do tratamento – especificando as imagens do rosto recolhidas), bem como o processo (a lógica) do tratamento automatizado dos dados biométricos no âmbito da tecnologia utilizada;

35. A CNPD chama também a atenção para o impacto que a subcontratação das operações ou de parte das operações de tratamento de dados biométricos pode ter na esfera jurídica dos cidadãos, sublinhado a inadmissibilidade, na ordem jurídica nacional, de subcontratações dos tratamentos de dados pessoais, inclusive biométricos, que impliquem ou comportem o acesso aos mesmos por Estados terceiros, em conformidade com a jurisprudência do Tribunal de Justiça da União Europeia, assinalando que as informações constantes da AIPD apontam no sentido dessa possibilidade, pelo que se recomenda que no Projeto de Portaria se acautele tal consequência.

36. Finalmente, assinala-se ainda:

- a. A dificuldade de conciliação do disposto no n.º 1 do artigo 2.º com o disposto no n.º 3 do artigo 7.º da Portaria, na redação dada pelo Projeto de Portaria, recomendando-se a ponderação do carácter opcional do fornecimento do endereço eletrónico, na parte final do n.º 1 do artigo 2.º, ou a explicitação no n.º 3 do artigo 7.º de que a possibilidade de alteração do número de telemóvel depende do fornecimento prévio, por parte do titular dos dados, de um contacto alternativo;
- b. A indicação no n.º 6 do artigo 6.º do «atendimento telefónico mediado», que não tem previsão no diploma legal que o Projeto de Portaria pretende regulamentar, e que traduz um novo meio de tratamento de dados pessoais, não se descortinando ter havido qualquer avaliação do risco específico colocado por via da utilização desse meio.

Lisboa, 3 de dezembro de 2021



Filipa Calvão (Presidente, que relatou)