CNPD
Comissão Nacional
de Proteção de Dados

PARECER/2021/99

I. Pedido

1. O Secretário de Estado da Presidência do Conselho de Ministros solicitou à Comissão Nacional de Proteção de Dados (CNPD) a emissão de parecer sobre o Projeto de Decreto-Lei n.º 956/XXII/2021, que «altera o sistema alternativo e voluntário de autenticação dos cidadãos nos portais e sítios na Internet da Administração Pública denominado Chave Móvel Digital».

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, 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

3. O Projeto de Decreto-Lei em apreço introduz três alterações principais na Lei n.º 37/2014, de 26 de junho, alterada por último pela Lei n.º 2/2020, de 31 de março: alarga o regime de utilização da Chave Móvel Digital (CMD) à autenticação aos sistemas eletrónicos e sítios na Internet, admite o recurso a funcionalidades de identificação biométrica do dispositivo móvel do cidadão e introduz a possibilidade de associação à CMD da tecnologia de reconhecimento facial.

4. Quanto à alteração assinalada em primeiro lugar, ela resulta da redação agora projetada para a alínea *a)* do artigo 1.º da Lei n.º 37/2014, assumindo-se que o regime, inicialmente previsto de autenticação dos cidadãos nos portais e sítios na Internet da Administração Pública, se estenda agora a quaisquer portais e sítios na Internet, portanto, também aos da responsabilidade de entidades privadas – embora, em rigor, o n.º 11 do artigo 2.º da mesma lei já admitisse a possibilidade de regulação da utilização da CMD como meio de autenticação em sítios na Internet.

5. A esta alteração soma-se a possibilidade de a autenticação poder ser concretizada por recurso a funcionalidades de identificação biométrica do dispositivo móvel do cidadão, nos termos enunciados na alínea *d)* do n.º 1 do artigo 3.º da Lei n.º 37/2014, introduzida pelo Projeto.

6. A mesma funcionalidade está prevista para a assinatura eletrónica qualificada, de acordo com a projetada alínea *d)* do n.º 1 do artigo 3.º-A da Lei n.º 37/2014.

i. A tecnologia de reconhecimento facial associada à CMD e a relevância da AIPD

7. Na perspetiva da tutela dos direitos, liberdades e garantias dos cidadãos no âmbito de tratamento de dados pessoais, merece especial atenção o novo regime de associação da tecnologia de reconhecimento facial à CMD para efeito da sua obtenção, previsto na nova redação do artigo 2.º, n.º 6, alínea *e)*, e n.ºs 17 a 19 da Lei n.º 37/2014.

8. A primeira observação que, a este propósito, cabe fazer prende-se com a indispensabilidade de um estudo de impacto sobre a proteção de dados pessoais decorrente deste novo tratamento de dados para, desde logo, permitir a tomada de opções no plano legislativo – cf. n.º 4 do artigo 18.º da Lei n.º 43/2004, de 18 de agosto, introduzido pela Lei n.º 58/2018, de 8 de agosto (Lei da Organização e Funcionamento da CNPD).

9. E se é certo que, ainda que a pedido da CNPD, foi entretanto enviada uma avaliação de impacto sobre a proteção de dados (AIPD) relativa ao sistema da CMD, essa avaliação reporta-se apenas a parte dos tratamentos de dados pessoais a que se refere o Projeto, sendo omisso quanto à utilização das funcionalidades de identificação segura biométrica como segundo fator de autenticação. Deste modo, a AIPD apresentada peca por não fornecer uma efetiva explicação das operações de tratamento de dados pessoais e uma avaliação dos riscos delas decorrentes em termos suficientes para uma decisão ponderada, por parte dos titulares do poder político-legislativo, sobre o enquadramento jurídico regulatório a dar aos novos tratamentos de dados pessoais.

10. Aliás, todo o processo em volta da regulação da utilização desta tecnologia para efeito de tratamento de dados pessoais é expressão da persistência num caminho que não é seguramente o desejável num Estado de Direito: o da elaboração de leis que se limitam a um mero reflexo da realidade de facto, prejudicando a função de orientação das condutas (dos cidadãos e, desde logo, da Administração Pública) que ao Direito e às normas legais é exigido.

11. Na verdade, a Agência para a Modernização Administrativa, I.P. (AMA), no âmbito de um processo de averiguações, declarou em 2020 não ter realizado qualquer AIPD relativa à tecnologia de reconhecimento facial, por, pretensamente, ter adquirido o licenciamento de um *software* sem que se encontrasse em implementação qualquer solução que fizesse uso do mesmo e apenas com a finalidade de avaliar a possibilidade de realizar a medida Simplex #50 e sem que se tivesse afadigado com o seu envio à CNPD quando, finalmente, a realizou.

12. E antes da eventual aprovação de diploma legislativo que legitimasse a utilização da tecnologia de reconhecimento facial – proibida nos termos do n.º 1 do artigo 9.º do RGPD e só excecionalmente admitida nos termos do n.º 2 do mesmo artigo –, o Gabinete Nacional de Segurança (GNS) fez publicar um despacho no

Diário da República[1], com regras – emitidas, portanto, por um órgão administrativo – juridicamente vinculativas para os responsáveis por tratamentos de dados pessoais na utilização da tecnologia de reconhecimento facial e que impactam nos direitos dos cidadãos, sem ter procedido à consulta prévia da CNPD e sem que se tivesse baseado numa AIPD. Correspondendo, obviamente, a um regulamento administrativo, este despacho estava sujeito às normas citadas supra, no ponto 2, assinalando-se ainda que as suas prescrições não têm natureza meramente técnica, incluindo mesmo regras sobre o tratamento de dados pessoais – como sucede com a previsão da possibilidade de conservação dos dados biométricos dentro de determinado prazo e com cumprimento de condições como a pseudonimização.

13. Para apenas em sede de procedimento legislativo, e após solicitação da CNPD, ter então sido apresentada a AIPD supra mencionada.

14. A CNPD insiste neste ponto porque a necessidade de acompanhamento prévio e subsequente, pelas autoridades de controlo, da regulação dos tratamentos de dados pessoais biométricos, especialmente com recurso à tecnologia de reconhecimento facial, tem sido bastamente destacada no plano europeu, atendendo ao impacto que os mesmos podem ter na vida das pessoas[2]. E insiste também porque, na subsequente apreciação das disposições constantes do Projeto, vai sublinhar algumas das incongruências entre estas e a referida AIPD, incongruências que poderiam ter sido evitadas tivesse sido outro o processo seguido.

ii. A insuficiência das normas do Projeto na definição dos tratamentos de dados e de garantias dos direitos

15. Relativamente ao regime legal dos 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 redação introduzida pelo Projeto, importa sublinhar que as normas em causa se limitam a pouco mais do que prever o tratamento, sem densificar os elementos e condições da sua realização, nem definir garantias dos direitos dos titulares dos dados.

16. Com efeito, não se define, desde logo, quem é o responsável pelo tratamento de dados pessoais. Note-se que a indicação, que consta, na versão ainda vigente, 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

[1] Cf. Despacho n.º 2705/2021, de 11 de março, relativo à «Identificação de pessoas físicas através de procedimentos de identificação à distância com recurso a sistemas biométricos automáticos de reconhecimento facial».

[2] Cf, por exemplo, as orientações do Conselho da Europa sobre reconhecimento facial: Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data – Convention 108, *Guidelines on Facial Recognition*, de 28 de janeiro de 2021, p. 8, acessível em https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3

quem é o responsável pelo tratamento de dados, nos termos enunciados na alínea 7) do artigo 4.º do RGPD[3], e nada diz sobre esta nova operação de tratamento de dados pessoais.

17. Acresce que não se definem os dados pessoais objeto de tratamento e, especificamente, não se 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): 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 compreende também as minúcias biométricas, se eventualmente a imagem do rosto que consta do cartão de cidadão (a que apenas se faz referência implícita no n.º 19 do artigo 2.º, quando se prevê a recolha da imagem do cartão de cidadão). Note-se que na AIPD (cf. 5.1.1.3. e 5.1.5.) se prevê a recolha de *selfie* e a recolha de fotografia do rosto e do respetivo *template* biométrico.

18. Aliás, o descrito nessas normas não parece coincidir e, portanto, não parecer dar cobertura legal às operações sobre dados pessoais descritas na AIPD apresentada – repare-se que só no n.º 19 do artigo 2.º se fala da «imagem do cartão de cidadão», que vem caracterizada, na AIPD, como correspondendo à fotografia de frente e verso do cartão de cidadão, portanto com todos os dados pessoais visíveis neste. Esta é uma das incongruências que deve ser corrigida.

19. Acresce que não há, no Projeto, qualquer explicação do processo de tratamento dos dados pessoais, para além da referência à comparação das enigmáticas *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* (cf. n.º 17 do artigo 2.º). Quando na AIPD (cf. 5.1.13 e 5.1.1.3.) se descreve uma outra operação comparativa biométrica entre a fotografia visível no cartão de cidadão e a constante daquele sistema de informação e se refere também a *utilização de algoritmos de Deep Learning para verificação da veracidade do Cartão de Cidadão*.

20. Ora, por razões que se prendem com a previsibilidade para os cidadãos dos tratamentos de dados pessoais a realizar pela Administração Pública, os diplomas legais devem definir os principais elementos do tratamento, entre os quais constam o responsável pelo tratamento, os dados objeto de tratamento 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*. Mais ainda quando o tratamento se fundamenta, de acordo com o

[3] 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.

determinado no Projeto, no consentimento do titular dos dados – cf. n.ºs 17 e 19 do artigo 2.º, introduzidos pelo Projeto.

21. Recorda-se que – aliás, também de acordo com as regras gerais de Direito – o consentimento pressupõe que a vontade manifestada seja livre e informada, para o que é essencial a prestação de informação clara quanto às operações sobre os dados pessoais – cf. alínea 11) do artigo 4.º do RGPD.

22. 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. Acresce que o Projeto nada diz sobre a tecnologia para deteção de vida e, como se referiu supra, ponto 19, na AIPD se afirma a utilização de algoritmos de *Deep Learning* para verificação da veracidade do cartão de cidadão.

23. 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 se corre o risco de, em concreto, se pretender que tal informação decorre já da lei 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 revela são escassos para a plena compreensão do mesmo e das suas implicações.

24. Até porque, quanto a uma das finalidades previstas para o tratamento (no n.º 19 do artigo 2.º), não é a mera remissão para uma «política de retenção de dados» que garante o direito de informação expressamente imposto no citado artigo 13.º do RGPD.

25. Ademais, a remissão para portaria governamental, constante do n.º 14 do artigo 2.º, da *regulamentação necessária para o desenvolvimento e segurança a infraestrutura da CMD* manifestamente não é, no contexto do tratamento de dados biométricos por recurso a tecnologia de *Deep Learning*, suscetível de substituir a definição dos elementos essenciais desse tratamento na sede própria, que é a lei, quando em causa está a finalidade última de autenticação de cidadãos perante entidades públicas e privadas.

26. Entende, por isso, a CNPD que deve definir-se, com mais detalhe no texto do Projeto de Decreto-Lei, 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, para que o cidadão possa estar suficientemente informado para o efeito de emitir o seu consentimento.

27. Ainda a respeito das omissões do Projeto quanto a este tratamento de dados biométricos, importa referir que os prazos de conservação dos dados pessoais devem estar definidos também no diploma legislativo e com exatidão, por aqui não poderem sobrar dúvidas quanto ao período durante o qual é necessária a sua conservação.

28. Com efeito, dir-se-ia que a fórmula utilizada no n.º 18 do artigo 2.º, de que as imagens do rosto são eliminadas após a conclusão do procedimento de obtenção da CMD, não esclarece o cidadão – este desconhece se esse é o momento em que conclui a validação dos elementos necessários à emissão da CMD, ou se é o da entrega da CMD. Entretanto, assinala-se que na AIPD se refere a eliminação automática *diária* da fotografia do rosto e do respetivo *template* biométrico. Acresce que, quanto à fotografia de frente e verso do cartão de cidadão e dos dados pessoais neles visíveis, se afirma na AIPD (cf. 5.1.11.) ficar conservada por 30 dias, de acordo com o estatuído no Despacho do GNS citado supra, no ponto 12. Portanto, mais uma vez, o que a norma legal dispõe não coincide com a descrição do sistema constante da AIPD apresentada.

29. De todo o modo, afigura-se essencial que no n.º 18 do artigo 2.º se estenda a eliminação automática a todos os dados pessoais recolhidos nessa operação e não apenas das imagens do rosto. Assim, e para pleno cumprimento da alínea *e)* do n.º 1 do artigo 5.º do RGPD, recomenda-se a especificação de que todos os dados pessoais recolhidos para a emissão da CMD são automaticamente eliminados após a validação dos elementos necessários para o efeito.

30. Ainda a respeito dos prazos de conservação, sugere-se a alteração da redação do n.º 9 do artigo 2.º. Aí se proíbe o *registo permanente* de todas as interações dos cidadãos com a Administração Pública ou outras entidades processadas através de CMD, quando, em rigor, o que o legislador parece querer proibir é o registo *integral* das autenticações. Na verdade, a Portaria n.º 77/2018, de 16 de março, na sua versão atual, prevê no artigo 12.º um ano como período de conservação para as autenticações com a CMD. Ou seja, existe em rigor um registo *permanente*, mas não integral, das autenticações enquanto a CMD está ativa, que vai sendo atualizado ao longo do tempo.

31. Em qualquer circunstância, não é razoável que os limites temporais de conservação dos dados pessoais relativos à utilização da CMD para autenticação perante entidades públicas e privadas não estejam hoje definidos na lei, por serem elementos essenciais do tratamento dos dados pessoais através de CMD. Recomenda-se, por isso, que a definição dos prazos de conservação desta informação pessoal seja introduzida na Lei n.º 37/2014.

iii. O recurso à videoconferência para adesão à CMD e confirmação de identidade

32. Ainda entre os meios alternativos de obtenção da CMD, o Projeto introduz no artigo 2.º, n.º 6, alínea *f)*, a possibilidade de a solicitação ocorrer por videoconferência, *mediante prévia confirmação de identidade, nos termos a definir na portaria prevista no n.º 14*.

33. A CNPD não questiona a possibilidade de recurso a um tal mecanismo, mas insiste, também a este propósito, ser imperiosa uma maior densificação normativa no plano legislativo, já que, tal como se apresenta, a alínea *f)* do n.º 6 do artigo 2.º não oferece qualquer orientação quanto à regulamentação administrativa, desde logo, no que diz respeito às garantias dos direitos dos cidadãos.

34. Não pode, pois, esta disposição legal limitar-se à mera delegação em regulamento administrativo numa matéria que tanto impacto tem na identidade dos cidadãos, na sua subsequente autenticação e nos diferentes atos jurídicos em que essa autenticação é necessária.

iv. A reutilização dos dados biométricos para outra finalidade

35. O n.º 19 introduzido pelo Projeto no artigo 2.º prevê ainda a recolha da imagem do cartão de cidadão pela AMA, IP., e o seu armazenamento por 10 dias, para efeitos de desenvolvimento evolutivo da CMD, mediante consentimento prévio do cidadão.

36. Em causa estará a reutilização da *imagem do cartão de cidadão* para uma finalidade distinta: o *desenvolvimento evolutivo da CMD*.

37. Logo se suscita a dúvida se por *imagem do cartão de cidadão* se pretende referir a fotografia do cidadão apresentada no cartão ou se a imagem de todo o cartão, portanto, compreendendo os dados pessoais visíveis neste documento de identificação. E se o tratamento poderá compreender também as correspondentes minúcias do rosto do cidadão. Reitera-se aqui a nota, deixada supra no ponto 18, de que a AIPD parece pressupor ser esta a reprodução de frente e verso do cartão de cidadão – o que, a confirmar-se, poderá ser desnecessário e excessivo para a finalidade pretendida, salvo se estiver relacionada não apenas com o aperfeiçoamento do algoritmo de reconhecimento facial, mas também com o aperfeiçoamento do algoritmo de verificação do cartão de cidadão. Por isso, sob pena de violação do princípio da minimização dos dados pessoais, consagrado na alínea *c)* do n.º 1 do artigo 5.º do RGPD, deve ser alterada a redação do n.º 19 do artigo 2.º, limitando o tratamento ao dado imagem do rosto ou explicitando a finalidade e o âmbito do novo tratamento.

38. Continuando no pressuposto de que por *imagem do cartão de cidadão* se pretende referir a reprodução do cartão de cidadão, frente e verso, a previsão na norma legal de que *os dados armazenados [...] não ficam*

associados ao cidadão suscita a maior perplexidade. Aliás, não bastasse o facto de os diferentes elementos de identificação do cidadão estarem visíveis nessa imagem, mesmo que estivesse 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[4].

39. De todo o modo, pretende-se realizar testes sobre dados pessoais reais, e também biométricos, para melhorar o algoritmo, com o consentimento a prestar pelo cidadão com base numa informação que, logo nos termos da sua designação *"política de retenção de dados"*, peca por insuficiente. Isto porque não são apenas a recolha e conservação dos dados pessoais que estão em causa; mais do que isso, há criação de uma base de dados para análise desses dados pelo algoritmo de *Deep Learning*.

40. Assim, tem a lei de explicitar em que consiste o tratamento de dados pessoais que está a prever, nos seus elementos principais, pois, além do prazo previsto, a caracterização do tratamento que o n.º 19 do artigo 2.º faz é inexata. Desde logo, imporá que se defina que dados pessoais são tratados (apenas a fotografia do rosto? também as correspondentes minúcias? os demais dados constantes do cartão de cidadão visíveis na imagem do mesmo?); e quais são as exatas operações de tratamento a que estão sujeitos.

41. Quanto a este último ponto, sublinha-se que *a recolha e a conservação* da imagem do cartão de cidadão, *per se,* não permitem realizar a finalidade declarada, pelo que, se a norma legal nada mais disser, só pode concluir-se pela falta de adequação do tratamento para a finalidade de «desenvolvimento evolutivo da CMD» e, nessa medida, pela manifesta desproporcionalidade da sua previsão legal.

42. A isto acrescem questões de proteção de dados que a norma não acautela de todo.

43. Não se estabelecem quaisquer regras orientadoras relativas ao local de armazenamento dos dados pessoais, sobretudo dos *templates* biométricos, desde logo, se a base de dados é conservada diretamente pelo responsável pelo tratamento – que, de acordo com a redação apresentada, aparenta ser a AMA, IP – ou se há possibilidade de subcontratação desta operação de tratamento de dados.

44. Recordando que em causa estão dados biométricos, especialmente protegidos por força do artigo 9.º do RGPD, pelo risco que o acesso e utilização indevida implica para a esfera jurídica e para a vida dos respetivos cidadãos, a CNPD alerta para a relevância de o legislador nacional equacionar a opção de exigir a conservação

[4] Não se compreendendo, por isso, a previsão desta condição para a conservação dos dados biométricos no citado Despacho do GNS (cf. Anexo A, 5.3.1.3.)

destes dados em território nacional – já que o responsável por esse tratamento é uma entidade pública administrativa – e de permitir ou excluir a possibilidade de subcontratação (aspeto que se desenvolverá infra, pontos 47 e ss.).

45. A única exigência de segurança dos dados pessoais que o preceito legal em causa prevê é a cifragem da imagem do cartão de cidadão. 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.

46. Pelas razões expostas, a CNPD recomenda a revisão do n.º 19 do artigo 2.º, prevendo-se específica e expressamente os dados pessoais tratados e as operações de tratamento a realizar, e definindo-se ainda regras relativas à criação e armazenamento desta base de dados biométricos, quer quanto à sua localização, quer quanto à direta responsabilização pela mesma.

v. Subcontratação

47. Finalmente, importa aqui destacar a questão já aflorada da 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. 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.

48. A hipótese de a entidade pública responsável pelo tratamento subcontratar um terceiro – *v.g.*, uma empresa privada – 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.

49. Entre tais questões apresenta-se, em primeira linha, a da localização da base de dados – se os dados ficam armazenados em território nacional, ou em território de um Estado-Membro da União, ou ainda em território de um Estado terceiro que ofereça um nível adequado de proteção dos dados. Se à luz do RGPD, qualquer destas soluções é admissível, não é indiferente, ainda assim, a questão numa perspetiva de opção política e de opção de cada cidadão.

50. Na verdade, mesmo na hipótese de essa base de dados biométricos estar situada em território de um Estado-Membro da União ou de um Estado terceiro que ofereça um nível adequado de proteção, é essencial garantir que a empresa subcontratante (ou subsubcontratante) não se encontra sujeita a regras jurídicas vinculativas de um Estado terceiro que possam afetar a proteção garantida no território onde está alojada a

base de dados – é o que sucederá, por exemplo, se a empresa onde está alojada a base de dados biométricos integrar um grupo societário cuja casa-mãe está sediada num Estado terceiro com regras jurídicas que a vinculam a disponibilizar às 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).

51. A CNPD deixa este alerta porque na AIPD apresentada (cf. 5.1.13 e 5.1.17) se refere a subcontratação do tratamento descrito no ponto 47 (com dados biométricos e acesso à base de dados ciclo de vida do cartão de cidadão) a uma empresa portuguesa que tem a plataforma e a base de dados alojada numa outra empresa com sede na Irlanda, a qual, por seu turno, integra um grupo societário (*Amazon*) cuja casa-mãe está sediada nos Estados Unidos da América. Ora, esta situação, tendo em conta a jurisprudência europeia citada, salvo demonstração da adoção de medidas suplementares de proteção, não é admissível nos termos do RGPD.

III. Conclusão

52. A CNPD entende que um diploma legislativo que pretende regular o reconhecimento facial no contexto da utilização da Chave Móvel Digital, porque em causa está o tratamento de dados biométricos com recurso a tecnologias de Inteligência Artificial de redes neuronais profundas, tem de definir com mais 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.

53. Assim, e com os fundamentos desenvolvidos supra, em II, a CNPD recomenda:

a. A revisão da alínea *e)* do n.º 6 e os n.ºs 17 e 18 do artigo 2.º da Lei n.º 34/2017, introduzidos pelo Projeto de Decreto-Lei, identificando-se os 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;

b. A especificação, no artigo 2.º da Lei n.º 34/2017, do prazo de conservação dos dados pessoais recolhidos para a emissão da CMD e a definição na mesma lei dos prazos de conservação das utilizações da CMD para autenticação dos cidadãos perante a Administração Pública e outras entidades, em pleno cumprimento da alínea *e)* do n.º 1 do artigo 5.º do RGPD;

c. A revisão do n.º 19 do artigo 2.º, sobre a recolha e armazenamento da imagem do cartão de cidadão pela AMA, IP., para efeitos de «desenvolvimento evolutivo da CMD», prevendo-se específica e expressamente os dados pessoais tratados e as operações de tratamento em vista, bem como definindo-se regras relativas à criação e armazenamento desta base de dados biométricos, quer quanto à sua localização, quer quanto à direta responsabilização pela mesma.

54. No que diz respeito à confirmação de identidade por videoconferência, a CNPD recomenda a densificação da alínea *f)* do n.º 6 do artigo 2.º, já que esta disposição não oferece qualquer orientação quanto à regulamentação administrativa por portaria, desde logo, no que diz respeito às garantias dos direitos dos cidadãos.

55. Por fim, a CNPD chama a atenção para a inadmissibilidade, na ordem jurídica nacional, de subcontratações dos tratamentos de dados pessoais, inclusive biométricos, que previnam o acesso aos mesmos por Estados terceiros, em conformidade com a jurisprudência do Tribunal de Justiça da União Europeia.

Aprovado na reunião de 22 de julho de 2021

Filipa Calvão (Presidente)