ASSEMBLEIA DA REPÚBLICA
Comissão de Apoio às Comissões
CACDLG

NU: 691063
Ent: 1592/1.ª-CACDLG-XIV/2021
de 08/11/2021

PARECER/2021/143

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 111/XIV/2.ª (GOV), que «Regula a utilização de sistemas de vigilância por câmaras de vídeo pelas forças e serviços de segurança».

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 44.º da Lei n.º 59/2019, de 8 de agosto, bem como pela alínea *c)* do n.º 1 do artigo 57.º e pela alínea *b)* do n.º 3 do artigo 58.º 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. A Proposta de Lei em apreço tem por objeto regular a utilização de sistemas de videovigilância pelas forças e serviços de segurança, procedendo à revogação da Lei n.º 1/2005, de 10 de janeiro, alterada por último pela Lei n.º 9/2012, de 23 de fevereiro (doravante, Lei n.º 1/2005). Como se refere na Exposição de Motivos, «[…] os avanços tecnológicos, que motivaram alterações significativas no que diz respeito às características técnicas dos sistemas que o mercado oferece em cada momento, exigem que o quadro legal seja adaptado às soluções técnicas hoje existentes».

4. Neste quadro, a Proposta de Lei alarga, não apenas o tipo de meios em que podem ser incorporadas câmaras de vídeo, como também as finalidades a prosseguir com a sua utilização e o próprio objeto de incidência, que vai além do espaço público, passando a abranger também áreas do domínio privado destinadas à circulação de pessoas, veículos, navios e embarcações. Também regula o «acesso pelas forças e serviços de segurança aos sistemas privados de vigilância, instalados em locais públicos ou privados de acesso ao público» (cf. Exposição de Motivos). A que acresce a permissão, sem condicionantes ou limites, da utilização de tecnologias de inteligência artificial, numa redação que permite a utilização de tecnologias de reconhecimento facial em espaço público ou privado de acesso ao público.

i. Considerações gerais

5. Sem se curar, por ora, da análise de cada uma destas alterações, começa-se por se destacar que este múltiplo alargamento da utilização de sistemas de videovigilância traz consigo o risco evidente de permitir uma utilização não adequada, arbitrária ou excessiva, quando não seja acompanhada de um regime legal bem densificado que preveja as condições da utilização de cada tipo de meio utilizado para captar e gravar imagens e som, e as respetivas salvaguardas, tendo em conta os específicos riscos ou impactos que cada um deles implica sobre os direitos fundamentais dos cidadãos. E é precisamente essa a maior lacuna desta Proposta de Lei.

a. Ausência de regras precisas sobre os tratamentos de dados pessoais, em especial de garantias dos direitos fundamentais

6. Na ânsia de cobrir todas as situações que na última década teriam, na perspetiva das forças e serviços de segurança, justificado a utilização de câmaras de vídeo e as novas tecnologias que potenciam a sua utilização, na Proposta preveem-se todos os equipamentos e tecnologias hoje disponíveis, quase numa lógica alternativa, como se não houvesse diferença de impacto nos direitos dos cidadãos. E elencam-se finalidades para a sua utilização, de modo indiferenciado, quando para a prossecução de parte delas apenas se revelarão aptos alguns tipos de meios de incorporação de câmaras, de entre os que aqui vêm previstos.

7. Ora, num Estado de Direito democrático não é admissível a mera previsão genérica de utilização de sistemas de videovigilância, em especial com recurso a tecnologias que potenciam os seus efeitos, sem a especificação de condições, limites e critérios necessários a garantir a sua idoneidade para prossecução de finalidades de interesse público, mas também imprescindíveis para assegurar que a afetação dos direitos fundamentais ocorra na medida do estritamente indispensável e sem excesso.

8. Recorda-se que a utilização de sistemas de videovigilância em espaço público representa sempre uma ingerência sobre os direitos fundamentais, máxime dos direitos ao respeito pela vida privada e familiar e à proteção de dados pessoais, consagrados nos artigos 26.º e 35.º da Constituição da República Portuguesa, bem como nos artigos 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia. Também a vida privada e familiar merece proteção explícita no artigo 8.º da Convenção Europeia dos Direitos Humanos, sendo conhecida a jurisprudência do Tribunal Europeu dos Direitos do Homem a exigir que as medidas legislativas restritivas daqueles direitos, sobretudo no contexto da atividade policial, tenham o grau de precisão necessário para assegurar a previsibilidade dos seus efeitos e demonstrem ser adequadas, necessárias e proporcionais à salvaguarda de valores comunitários essenciais enunciados no n.º 2 daquele artigo 8.º.

9. A ausência de um regime legal preciso, com a definição das condições e limites da utilização de cada um dos tipos de meios técnicos disponíveis hoje para a captação e gravação de imagens, prejudica a previsibilidade

imprescindível num diploma legal que, em si mesmo, com a intenção de tutelar valores públicos de segurança e direitos fundamentais, prevê e implica restrições intensas em outros direitos fundamentais. E representa um "cheque em branco" à intrusão na vida privada dos cidadãos, como se o facto de se encontrarem em espaços público ou de acesso público implicasse a automática negação dessa dimensão humana fundamental. Mais, permitindo ainda, também com grande abertura, *rectius*, com nula densificação normativa, a utilização neste contexto de tecnologias de inteligência artificial, em especial de reconhecimento facial, na aparente ignorância dos riscos de erro e de discriminação que da sua utilização podem resultar.

10. É este "cheque em branco" que a Proposta de Lei representa que suscita na CNPD a maior das apreensões. Sobretudo tendo em conta as efetivas condições de utilização de sistemas de videovigilância pelas forças e serviços de segurança que a CNPD tem verificado, no exercício da sua atividade inspetiva, as quais revelam que os sistemas de videovigilância já existentes, seja pela ausência de regras e critérios claros e uniformizados quanto à sua utilização, seja pelo desrespeito da parca regulamentação existente, seja pela falta de meios para o controlo efetivo, por parte das forças de segurança, dos equipamentos e da sua utilização, não se têm mostrado aptos à prossecução das finalidades visadas.

11. Assim, antes de se analisar cada uma das previsões legais que suscitam reservas na perspetiva da tutela dos direitos fundamentais dos cidadãos no âmbito do tratamento de dados pessoais, a CNPD entende ser útil para os titulares do poder político-legislativo elencar alguns exemplos que revelam o estado atual dos tratamentos de dados realizados no contexto da utilização dos sistemas de videovigilância ao abrigo da Lei n.º 1/2005, o que faz em seguida.

b. O funcionamento de sistemas de videovigilância já autorizados

12. A CNPD tem vindo a acompanhar tratamentos de dados pessoais realizados por sistemas de videovigilância em espaço público pela Polícia de Segurança Pública (PSP) e o impacto do recurso a novas ferramentas disponíveis em função da evolução tecnológica, cuja utilização tem sido autorizada pelo membro do Governo com competência delegada na matéria. As situações que aqui são apresentadas vêm descritas nos relatórios intercalares da CNPD quanto às inspeções já efetuadas, prevendo a CNPD realizar ainda novas inspeções tendo em conta que têm sido, entretanto, emitidas novas autorizações que legitimam a utilização de diferente tecnologia. Logo que conclua estes procedimentos de acompanhamento, a CNPD emitirá uma pronúncia sobre os tratamentos de dados pessoais verificados, da qual será dado conhecimento aos titulares do poder político-legislativo.

13. Assim, até ao momento a CNPD verificou que os tratamentos de dados pessoais realizados por tais sistemas de videovigilância não cumprem muitos dos requisitos previstos quer em lei, quer nas portarias que a Lei n.º

1/2005, quer ainda nos próprios despacho autorizativos dos sistemas. Em seguida apresentam-se algumas das inconformidades detetadas.

14. Começa-se por destacar que, apesar da PSP ser o responsável pelo tratamento dos sistemas de videovigilância inspecionados, os contratos de instalação e manutenção, preventiva e corretiva, destes sistemas são celebrados pelos municípios e pelas empresas prestadoras dos serviços, sem qualquer intervenção da PSP e sem que esta conheça o seu teor. Deste modo, por não ser parte destes contratos, a PSP não tem legitimidade para exigir qualquer apoio, correção, ou atualização dos sistemas.

15. Os contratos analisados não contêm quaisquer regras de proteção de dados, como impõe a lei, nem obrigam a que os trabalhadores das empresas que prestam serviços de apoio ao sistema, por regra com perfis de administração, estejam credenciados pelo Gabinete Nacional de Segurança.

16. Acresce que todos os perfis de administração do sistema, que permitem realizar todas as operações, portanto, também as de maior sensibilidade, não pertencem a agentes da PSP, que os desconhecem, mas antes a pessoas das empresas prestadoras de serviços.

17. Verificou-se ainda que o *software* das máquinas e o *firmware* das câmaras de videovigilância não estavam atualizados, mantendo as versões do momento da instalação, quando essas atualizações são essenciais para garantir a segurança do sistema.

18. Quanto aos sistemas de controlo de acesso às salas de visualização e *data center* verificou-se, num dos casos, que estava avariado e, num outro, que o sistema de controlo de acesso ao *data center* estava desligado. Mas, ainda que estivessem todos ativos, concluiu-se que tais sistemas apresentam grandes fragilidades; constatou-se que no acesso são utilizados cartões com tecnologia suscetível de clonagem por aplicações descarregáveis gratuitamente na Internet e que não há um segundo fator de autenticação.

19. Num dos sistemas inspecionados, a sala utilizada como *data center* (com controlo de acessos desligado) era o único caminho de passagem para o vestiário dos agentes, o que demonstra a falta de condições das instalações para garantir a segurança do sistema.

20. Também num dos sistemas de videovigilância verificado, a rede do sistema de videovigilância não estava segregada, sendo partilhada com a rede do Município e os bastidores que ligavam as câmaras a essa rede estavam colocados no chão (do espaço público), tornando-os especialmente vulneráveis a acessos indevidos e ataques.

21. No que diz respeito aos registos de auditoria, verificou-se que os mesmos não são fidedignos. Com efeito, não permitem identificar quem fez uma operação no sistema de videovigilância (*v.g.*, acesso, eliminação de filtros de privacidade), quando o fez e que tipo de operação efetuou.

22. Os registos de auditoria não são objeto de análise e não existe qualquer alarmística para situações fora de padrões de utilização normal. Com efeito, foram detetados pela CNPD acessos por utilizadores que não estavam autenticados no sistema, nem de serviço (escala), que configuravam um comportamento típico de ataque, sem que a PSP ou a empresa contratada o tivessem detetado.

23. Nenhum dos sistemas tinha plano de *Disaster Recovery*, nem sequer *backups*.

24. Os sistemas não estavam sincronizados com a hora legal. Os dispositivos dos sistemas (câmaras e postos de trabalho) não apresentavam a mesma hora.

25. Nos sistemas inspecionados contatou-se que havia situações em que o barramento de locais privados (máscaras) não impedia a sua visualização, designadamente de portas, janelas e varandas.

26. Relativamente a um dos sistemas de videovigilância, a CNPD foi informada que as máscaras são configuradas manualmente pelo administrador do sistema, em cada câmara, num máximo de 24 retângulos, o que nem sempre permite cobrir todos os espaços privados a ocultar.

27. No mesmo sistema, a CNPD testou a opção de ativar/desativar máscaras pelo utilizador, verificando que as mesmas são apresentadas de acordo com os comandos dados. Mas constatou que estas operações não ficam registadas no *log* de modo identificável, *i.e.*, para além do já referido anteriormente, nem sequer o tipo de operação efetuada consta do *log* (registo de auditoria), impedindo qualquer auditoria, interna ou externa, à legitimidade das operações.

28. Ainda no mesmo sistema, constatou-se a instalação de *software* que, para ser utilizado, implica ligação à Internet, designadamente *FaceBook, Netflix, Receitas, Skype, Royal Revolt2, Twitter, TuneIn radio*, o que constitui uma incongruência num sistema que tem de funcionar em rede isolada. Independentemente de outras considerações, a simples existência e utilização deste tipo de *software* apresenta vetores de risco (*v.g., cookies, device fingerprinting*, código malicioso) inadmissíveis num sistema de videovigilância das forças de segurança.

29. Noutro sistema, encontrou-se instalado no servidor *software* para acesso à Internet (de Banda Larga TMN) e, no mesmo local, num dos postos de trabalho outros *software* para acesso à Internet (*Vodafone Mobile Broadband* e Banda Larga Móvel da MEO), facto que constitui um forte indício de o sistema ter estado ligado à Internet, o que importa mais uma vulnerabilidade para o sistema.

30. Num posto de trabalho, em pesquisas por ".jpg" e ".jpeg" nos discos, obtiveram-se listagens de pastas com imagens que totalizavam mais de 400 pastas e mais de 6000 ficheiros entre fotogramas e vídeos desde o início do funcionamento sistema.

31. Em síntese, o aqui sumariamente descrito revela que a utilização dos sistemas de videovigilância não cumpre as regras relativas à segurança e integridade dos tratamentos de dados pessoais e que a PSP não tem tido condições de facto, mas também jurídicas, para a sua utilização em conformidade com o quadro legal e regulamentar, não dispondo, desde logo, do indispensável domínio sobre os equipamentos e a sua utilização.

32. Tendo isto em conta, a opção vertida nesta Proposta de Lei de alargar e complexificar os sistemas de videovigilância com novas tecnologias, parece revelar o desconhecimento da realidade com que se debatem as forças e serviços de segurança no seu dia a dia no contexto da utilização de sistemas de videovigilância.

33. Analisa-se em seguida o articulado da Proposta de Lei, para destacar as deficiências que as diferentes normas revelam no que ao tratamento de dados pessoais diz respeito.

ii. Âmbito de aplicação da lei e finalidades dos sistemas de videovigilância

34. Logo no artigo 2.º da Proposta de Lei se determina que o nela disposto se aplica «aos sistemas de videovigilância instalados ou utilizados no espaço público ou em áreas do domínio privado destinadas à circulação pública de pessoas, veículos, navios e embarcações, quando devidamente autorizados, e para os fins previstos no artigo seguinte».

35. Quanto às finalidades dos sistemas de videovigilância elencadas no artigo 3.º da Proposta, as mesmas duplicaram em relação às atualmente definidas no artigo 2.º da Lei n.º 1/2005. Com efeito, além do alargamento da finalidade de proteção e de segurança dos animais, e da autonomização da finalidade de controlo de tráfego na circulação rodoviária (já acautelada no artigo 13.º da Lei n.º 1/2005), somam-se ainda as seguintes: *apoio à atividade operacional das forças e serviços de segurança em operações policiais complexas, nomeadamente em eventos de dimensão ampla ou internacional ou de outras operações de elevado risco ou ameaça; resposta operacional a incidentes de segurança em curso; controlo de tráfego e segurança de pessoas, animais e bens na navegação marítima e fluvial, bem como prevenção e repressão das infrações aos regimes vigentes em matéria de navegação e proteção do meio marinho; controlo de circulação de pessoas nas fronteiras; apoio em operações de busca e salvamento.*

a. As finalidades de prevenção e repressão criminal *vs* as finalidades de mera ordenação social

36. Não questionando as novas finalidades aqui consideradas, a CNPD não pode deixar de assinalar que, conforme se estatui no proémio do artigo, se se limita a utilização dos sistemas de videovigilância *apenas* «para a *prossecução dos fins previstos na Lei de Segurança Interna*, aprovada pela Lei n.º 53/2008, de 29 de agosto, na sua redação atual» [destacado nosso], então não se compreende que aí venha enumerado o *controlo de tráfego* (na circulação rodoviária e na navegação marítima e fluvial) e a *prevenção e repressão de infrações estradais e prevenção e repressão das infrações aos regimes vigentes em matéria de navegação* (cf. alíneas *g), h)* e *i)* do artigo 3.º da Proposta), que manifestamente ali não se encaixam. Recomenda-se, por isso, a reponderação do elenco das finalidades apresentado ou da referência expressa aos fins previstos na Lei de Segurança Interna.

37. A este propósito, importa ainda sublinhar que, se o objeto da Proposta de Lei é o de regular os tratamentos de dados pessoais decorrentes da utilização de sistemas de videovigilância no espaço público (e no espaço privado de acesso ao público) não apenas para finalidades de prevenção e repressão criminal, mas também para a prevenção e repressão de infrações de natureza estritamente contraordenacional e, bem assim, de controlo de tráfego e deteção e proteção contra incêndios florestais e rurais, então não pode esta Proposta limitar-se, quanto aos tratamento de dados, às remissões para a Lei n.º 59/2019, de 8 de agosto, devendo também integrar remissões para o RGPD e para a Lei n.º 58/2019, de 8 de agosto – referimo-nos às remissões constantes dos n.º 2 do artigo 2.º, n.º 5 do artigo 18.º, artigo 19.º, n.ºs 1 e 2 do artigo 22.º e artigo 27.º da Proposta.

38. Demais, ainda quanto às finalidades elencadas no artigo 3.º da Proposta, destaca-se a alteração substancial da redação da alínea relativa à finalidade de *proteção de pessoais, animais e bens em locais públicos ou de acesso público*, pois que agora a alínea *d)* alarga as circunstâncias que permitem afirmar a necessidade de proteção (por comparação com a Lei n.º 1/2005). Assim, aí se elencam as seguintes situações: *i. Elevada probabilidade de ocorrência de factos qualificados pela lei como crime; ii. Elevada circulação ou concentração de pessoas; iii. Ocorrência de facto suscetível de perturbação da ordem pública.*

39. Ora, é duvidoso que o mero facto de, num dado local público ou de acesso público, haver *elevada circulação ou concentração de pessoas* seja, *per se*, suficiente para afirmar a necessidade de proteção de pessoais, animais e bens. Não se vê onde esteja o perigo ou ameaça séria para a integridade das pessoas, animais ou bens por força da situação assim caracterizada. Até pela imprecisão do adjetivo "elevada" que não permite compreender se aí cabem as situações excecionais de circulação e concentração de pessoas por ocasião de um determinado evento (*v.g.*, a noite de S. João na cidade do Porto) ou se também cabem as situações normais e recorrentes de circulação de pessoas nas ruas de uma populosa cidade.

40. Acresce que, no âmbito dessa mesma finalidade, o pressuposto *ocorrência de facto suscetível de perturbação da ordem pública* afigura-se ser demasiado amplo. Não pode ser uma qualquer perturbação da ordem pública a merecer a utilização de meios que podem revelar-se altamente intrusivos na esfera jurídica dos cidadãos que se encontram no espaço público ou mesmo em áreas privadas ainda que de acesso ao público. A restrição dos direitos fundamentais, máxime do direito ao respeito pela vida privada, que a utilização de um sistema de videovigilância implica, tem de estar justificado pela necessidade de salvaguardar um interesse comunitário importante ou um direito fundamental, não bastando um qualquer interesse de mera ordenação social. Essa é a razão por que a videovigilância no espaço público quando implique o tratamento de dados pessoais está ao serviço da prevenção e repressão criminais ou de salvaguarda da vida das pessoas (e agora dos animais) e, apenas em determinadas circunstâncias bem delimitadas, poderá servir as finalidades de prevenção e repressão de ilícitos de mera ordenação social – mas aqui, ainda assim, por se considerar estarem em causa dimensões humanas ou valores especialmente relevantes na sociedade.

41. De resto, é bom de ver que se o facto ilícito já ocorreu, a utilização da câmara não se apresenta como um meio adequado para o efeito de proteção de pessoas, animais e bens, não se vendo, pois, como possa constar esta finalidade assim delimitada do elenco daquelas que justificam, em abstrato, a instalação e utilização de sistemas de videovigilância.

42. Não é, pois, nem pode ser uma qualquer *perturbação da ordem pública* a legitimar a utilização de sistemas de videovigilância, tão-pouco pretensas sensações de insegurança. Deste modo, a CNPD considera deverem ser eliminados os incisos *ii.* e *iii*. da alínea *d)* do artigo 3.º, por traduzirem a extensão da utilização da videovigilância a situações em que não há efetiva necessidade de proteção, revelando-se assim uma medida legislativa restritiva dos direitos fundamentais ao respeito pela vida privada e à proteção dos dados pessoais desnecessária e excessiva, em violação do n.º 2 do artigo 18.º da Constituição da República Portuguesa (CRP).

43. De resto, deve ainda destacar-se que há finalidades descritas em termos que não facilitam a certeza e previsibilidade jurídicas quanto à sua verificação. É o caso da finalidade, prevista na alínea *c)* do artigo 3.º, de apoio à *atividade operacional das forças e serviços de segurança em operações policiais complexas*, cuja exemplificação se reconduz a *eventos de dimensão ampla ou internacional*, não sendo evidente se a *amplitude* da dimensão do evento respeita ao universo de pessoas que o compõem ou simplesmente à área espacial por ele coberta. Não obstante tratar-se de terminologia que o legislador já utilizou na Lei de Segurança Interna, o certo é que se trata de um conceito vago, pelo que melhor seria que, em vez de o replicar, ele fosse densificado. Destaca-se também que a finalidade de *resposta operacional a incidentes de segurança em curso*, enunciada na

alínea *f)* do artigo 3.º, não aparece suficientemente densificada para que tenha autonomia em relação às hipóteses previstas nas alíneas *a)* a *d)* do mesmo artigo 3.º.

b. Videovigilância das propriedades privadas

44. A CNPD assinala também que algumas das finalidades previstas no artigo 3.º da Proposta implicam ou podem implicar a captação de imagens de propriedades privadas, as quais não coincidem com o conceito utilizado no artigo 2.º da Proposta para definir o âmbito da respetiva aplicação («áreas do domínio privado destinadas à circulação pública de pessoas, veículos, navios e embarcações»).

45. É o que sucede, por exemplo, com a finalidade de *controlo de circulação de pessoas nas fronteiras,* prevista na alínea *j)* do artigo 3.º da Proposta. Tendo em conta a extensão da fronteira terrestre portuguesa e os meios que poderão ser utilizados para a prossecução desta finalidade (*v.g.,* aeronaves não tripuladas), sobram sérias dúvidas se ela é compatível com o âmbito de aplicação da Proposta de Lei ou se não deve a mesma ser delimitada às áreas onde se situam os postos de controlo fronteiriço. E, ainda assim, tendo em conta que no quadro do projeto europeu se criou um espaço de liberdade de circulação, dificilmente se compreende como lícita a finalidade de controlo de circulação nas fronteiras internas. Se o legislador aqui tem em vista somente as *fronteiras externas*, deve assim delimitar essa finalidade, para afastar qualquer dúvida quanto a uma eventual restrição de liberdades asseguradas no quadro jurídico europeu.

c. Ausência de delimitação das finalidades em função dos meios de vigilância utilizados

46. Em suma, o artigo 3.º multiplica as finalidades do tratamento de dados pessoais associado à utilização de sistemas de videovigilância, num esforço de abarcar todas as situações que até ao momento teriam justificado essa utilização. Mas como são múltiplos também os meios que apresenta para a execução dessa videovigilância, acaba por potenciar ou legitimar a utilização de meios que não são aptos para a prossecução dessas finalidades (ou que, sendo-o se revelam, à partida, excessivos, atendendo ao seu grau de intrusão na esfera privada dos cidadãos).

47. Melhor seria delimitar autonomamente as finalidades que certos tipos de meios – a consagrar-se, a final, a possibilidade da sua utilização – podem prosseguir, em especial no que diz respeito às aeronaves não tripuladas (*drones*) e às "câmaras de uso individual" (*bodycams*).

iii. Princípios aplicáveis à utilização de sistemas de videovigilância

48. O artigo 4.º prevê os princípios aplicáveis à utilização de sistemas de videovigilância, os quais, em rigor, se reduzem ao princípio da proporcionalidade nas suas diferentes vertentes, reproduzindo praticamente sem alterações o disposto no artigo 7.º da Lei n.º 1/2005.

49. Não obstante, porque a Proposta de Lei alarga substancialmente o âmbito e os meios a utilizar neste contexto, há disposições que devem ser reponderadas cuidadosamente.

50. É desde logo o caso da proibição de instalação de câmaras fixas em áreas que, apesar de situadas em locais públicos, sejam pela sua natureza destinadas a ser utilizadas em resguardo – cf. n.º 4 do artigo 4.º da Proposta. Na verdade, o aí disposto peca por defeito ao limitar a proibição às câmaras fixas, porque, a partir do momento em que o legislador pretende legitimar a utilização de aeronaves não tripuladas, não pode deixar de estender a mesma proibição a soluções técnicas suscetíveis de produzir (pelo menos) o mesmo impacto nos direitos fundamentais dos cidadãos do que a captação de imagens e som por via de câmaras fixas.

51. A CNPD recomenda, por isso, a reponderação da redação do n.º 4 do artigo 4.º da Proposta, insistindo na extensão deste regime à utilização de aeronaves não tripuladas.

52. Ainda sobre o artigo 4.º, convinha atualizar ou aperfeiçoar algumas das suas normas. Tenha-se aqui em vista, desde logo, o n.º 5 deste artigo, que apenas salvaguarda *o interior de casa ou edifício habitado ou sua dependência*, quando é certo que merece igual proteção o interior de estabelecimentos hoteleiros ou estabelecimento similares, de ginásios, e mesmo de edifícios destinados a escritórios, sobretudo quando em causa estejam compartimentos de uso individual (onde as pessoas passam mais tempo ativas – acordadas – do que na sua própria casa).

53. A CNPD recomenda, assim, que se atualize a redação do n.º 5 do artigo 4.º, estendendo a garantia nele prevista também ao interior de outros edifícios onde a mesma razão de proteção da privacidade se faz sentir com intensidade similar ou próxima (*v.g.*, estabelecimentos hoteleiros ou similares e escritórios).

iv. O regime jurídico das câmaras fixas

a. Limitação da transparência

54. Relativamente ao regime jurídico das câmaras fixas, previsto nos artigos 5.º e seguintes da Proposta de Lei, começa-se por assinalar o encurtamento do prazo para a emissão do parecer da CNPD e a proibição de publicitação no parecer de alguns elementos relativos ao sistema de videovigilância quando em causa estejam *infraestruturas críticas, pontos sensíveis ou instalações com interesse para a defesa e a segurança*.

55. A CNPD chama a atenção para o facto de alguns dos elementos especificados no n.º 6 do artigo 5.º da Proposta, terem, nos termos da lei, de constar da autorização a emitir, a qual, por seu turno, é publicada no Diário da República. É especificamente o que sucede com a identificação do local e área abrangida pelo sistema e as características técnicas do equipamento utilizado – cf. alíneas *a)* e *d)* do n.º 1 do artigo 7.º da Proposta.

56. A este propósito, a CNPD sublinha ainda que a criticidade das infraestruturas ou a sensibilidade dos pontos ou instalações tem de ser devidamente assinalada no pedido de parecer, porque esta entidade não dispõe da informação para concluir pelo preenchimento de tais conceitos imprecisos, mas tem também de ser devidamente fundamentada, para que a CNPD possa, ainda numa lógica de controlo extrínseco de evidência, confirmar a verificação dos pressupostos da imposição legal de ocultação de informação no processo de publicitação dos seus pareceres.

b. A imprescindibilidade da avaliação do risco na instrução do pedido de autorização

57. No que diz respeito ao pedido de autorização, sublinha-se que é imprescindível, de acordo com a Lei n.º 59/2019, de 8 de agosto, que o mesmo seja acompanhado da avaliação de impacto sobre a proteção de dados pessoais.

58. Na verdade, a consulta prévia da CNPD, imposta no âmbito do procedimento autorizativo, pressupõe que tal obrigação tenha já sido cumprida, nos termos no n.º 1 do artigo 29.º da Lei n.º 59/2019, de 8 de agosto[1]. Note-se que o tratamento de dados pessoais associado à utilização de sistemas de videovigilância é sempre considerado *de elevado risco para os direitos, liberdades e garantias das pessoas*, por incidir *sobre uma grande quantidade de dados pessoais e afetar um grande número de titulares de dado,* como resulta do considerando 51 da Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril, diretiva que aquela lei transpôs para a ordem jurídica portuguesa – sendo certo que o disposto nesta lei não pode deixar de ser interpretado e aplicado em conformidade com a Diretiva. Por isso, tendo o responsável pelo tratamento o dever de realizar a avaliação de impacto e a CNPD o dever de emitir parecer sobre o tratamento de dados, afigura-se lógico que aquele seja um elemento a juntar na instrução do pedido de autorização.

59. Por isso mesmo, a CNPD considera essencial que seja acrescentada uma nova alínea ao n.º 1 do artigo 6.º da Proposta, exigindo que o pedido seja instruído com a avaliação de impacto sobre a proteção de dados pessoais. E que seja eliminado o n.º 5 do artigo 18.º da Proposta, por estar a restringir uma obrigação imposta pela citada Diretiva (a este ponto voltaremos). Mais se recomenda que a alínea que venha a ser introduzida neste

[1] E no artigo 35.º, n.º 3, alínea *c)*, do RGPD, quanto aos tratamentos de dados pessoais que vêm regulados nos artigos 12.º, 14.º e 15.º da Proposta de Lei.

n.º 1 sobre tal avaliação seja ainda especificamente acrescentada ao elenco constante do n.º 3 do artigo 10.º da Proposta de Lei (relativo à instrução de pedido relativo a câmaras portáteis).

c. A restrição da competência autorizativa do membro do Governo

60. Ainda quanto ao artigo 6.º, importa alertar para o absurdo de se limitar a competência do membro do Governo que tutela a força ou serviço de segurança requerente à verificação do disposto nos n.ºs 1, 2 e 3 do artigo 4.º da Proposta de Lei – onde se vincula a utilização de câmaras ao princípio da proporcionalidade, na vertente da adequação e da necessidade –, porque o cumprimento dos limites fixados nos n.ºs 4 a 6 desse artigo – relativos ao respeito específico pela privacidade – tem também de ser verificado por aquele órgão, enquanto titular do poder autorizativo, uma vez que são pressupostos legais, negativos, da autorização. E porque o parecer da CNPD, que tem de incidir sobre os n.ºs 4 a 6 do artigo 4.º (cf. n.º 3 do artigo 5.º da Proposta), é um mero ato jurídico opinativo, sem força jurídica vinculativa, que serve de apoio ao exercício da competência autorizativa do membro do Governo, portanto, serve de apoio à verificação do cumprimento desses pressupostos definidos no artigo 4.º – sendo especialmente relevante por criar no membro do Governo o dever de fundamentação caso decida em sentido diferente do parecer (cf. artigo 151.º, n.º 1, alínea *c)*, do Código do Procedimento Administrativo).

61. A CNPD recomenda, por isso, a reformulação do disposto no n.º 3 do artigo 6.º da Proposta, no sentido de não excluir da competência do membro do Governo a verificação dos pressupostos previstos nos n.ºs 4 a 6 do artigo 4.º, ainda que com o apoio no parecer da CNPD.

d. Redução dos prazos

62. Uma última nota, agora sobre prazos, sobretudo sobre o relativo à duração da autorização. No artigo 7.º, assinala-se a novidade de se fixar um prazo máximo de 5 anos (ao contrário do prazo de 2 anos da Lei n.º 1/2005), o que representa um alargamento substancial do mesmo.

63. Importa aqui ponderar, desde logo, que critérios poderão estar na base da previsão de um prazo máximo de 5 de anos, mais do dobro do atual, sendo certo que a Exposição de Motivos é quanto a tal omissa. Repare-se que o prazo de 2 anos, atualmente vigente, veio alterar o prazo inicialmente previsto na Lei n.º 1/2005, que era de 1 ano.

64. Recorda-se que esta legislação assentou no pressuposto de que, tanto as câmaras fixas, como as câmaras móveis, seriam usadas para atender a situações específicas e de certa excecionalidade que exigiam a videovigilância para um específico evento ou para fazer face a um determinado fenómeno. Se a extensão para 2 anos foi um primeiro sinal de simplificação da verificação de tais circunstâncias, a fixação de um prazo de 5 anos revela o abandono de qualquer juízo de excecionalidade ou de necessidade temporalmente delimitada da

videovigilância. Significa, pois, a assunção de que os sistemas de videovigilância devem existir independentemente da demonstração da sua necessidade, bastando-se com um juízo inicial (por vezes, sumário) sobre a proporcionalidade da sua utilização, desprezando a ingerência na vida privada das pessoas que tal significa.

65. De resto, este prazo prejudica a reavaliação atempada da necessidade da utilização de sistemas de videovigilância também tendo em conta que, por força da evolução tecnológica, os equipamentos técnicos e as medidas de segurança adotadas podem, num período tão extenso, tornar-se acentuadamente obsoletos.

66. A CNPD recomenda, por tudo isto, a reponderação do prazo máximo fixado no artigo 7.º da Proposta de Lei, por não encontrar motivos para a sua sustentação, quer face à imprescindível exigência de regular reavaliação da adequação, necessidade e proporcionalidade da utilização dos sistemas de videovigilância, quer face à tendencial obsolescência dos sistemas num período de tempo tão extenso.

67. Paralelamente, deve também ponderar-se se o prazo de 30 dias antes da caducidade da autorização para renovação do pedido não é insuficiente para garantir a consulta prévia da CNPD sempre que o pedido de renovação incorpore alterações em relação à autorização inicial, em especial considerando o prazo – também de 30 dias – de que a CNPD dispõe para a emissão do seu parecer.

68. Recomenda-se, por isso, a reponderação dos prazos fixados nos n.ºs 3 e 4 do artigo 7.º da Proposta de Lei.

v. Regimes excecionais e especiais

a. A instalação ou utilização de câmaras sem autorização prévia do membro do Governo

69. O artigo 9.º exceciona da necessidade de obtenção de autorização prévia a instalação de câmaras fixas, por decisão do dirigente máximo da força ou serviço de segurança, quando se verifiquem circunstâncias urgentes devidamente fundamentadas e que constituam um perigo para a defesa do Estado ou para segurança e ordem pública.

70. Exceção similar vem prevista no n.º 5 do artigo 10.º, quanto à utilização de câmaras portáteis, embora aqui os respetivos pressupostos legais sejam aligeirados, bastando-se com a fórmula «*quando não seja possível obter em tempo útil a autorização* [...]».

71. Em ambos os casos, se impõe a obtenção *ex post* da autorização, prescrevendo o dever de destruição do material gravado no caso de a autorização não ser emitida.

72. Este regime excecional estava previsto na Lei n.º 1/2005, mas apenas para a utilização de câmaras portáteis (cf. artigo 6.º desse diploma legal).

73. Assinala-se que, em comparação com o disposto no n.º 3 do artigo 6.º da Lei n.º 1/2005, que impõe a destruição do material gravado também no caso de, no âmbito do procedimento autorizativo ulterior, a CNPD emitir parecer negativo, na presente Proposta de lei o parecer da CNPD deixa de ter força vinculativa. São, pois, muitas as alterações introduzidas no procedimento excecional de utilização de câmaras portáteis sem autorização prévia, no sentido de aligeirar o procedimento e de retirar impacto à consulta prévia da CNPD. O que não pode deixar de suscitar apreensão, sobretudo porque neste regime das câmaras portáteis está também abrangido o tratamento de dados feito com recurso a câmaras incorporadas em aeronaves não tripuladas (vulgo, *drones*), como em seguida se focará.

74. Está, em todo o caso, em causa a utilização de câmaras fixas ou portáteis em que se dispensa o controlo prévio do membro do Governo, bastando-se com a decisão do dirigente máximo da força de segurança, com base em pressupostos especialmente imprecisos. A experiência demonstra que as *circunstâncias urgentes* ou a impossibilidade de obtenção *em tempo útil* da autorização acabam por se reportar a eventos agendados com bastante antecedência, em relação aos quais é desde cedo previsível a necessidade de vigilância, só pontualmente se invocando factos supervenientes reveladores da necessidade do recurso à videovigilância (*v.g.*, festividades em espaço público na passagem de ano, cortejos carnavalescos, jogos de futebol, cimeiras internacionais ou eventos similares, como a *Web Summit*).

75. A ausência de controlo prévio e o enfraquecimento do controlo *a posteriori*, por um lado, e a imprecisão dos pressupostos da utilização destes procedimentos excecionais, onde nem se faz expressa referência à *necessidade* da utilização de videovigilância, não pode deixar de causar apreensão quanto à aplicação em concreto destes preceitos legais.

b. A utilização de câmaras portáteis, em especial os *drones*

(i) Exclusão da consulta prévia à CNPD

76. Quanto ao procedimento de autorização da utilização de câmaras portáteis, regulado no artigo 10.º, importa destacar, desde logo, que em nenhum ponto desse artigo se remete para o regime de autorização previsto no artigo 5.º da Proposta (mas já contém uma remissão parcial para o artigo 6.º, relativo aos elementos que devem instruir o requerimento). Tal omissão permite a interpretação de que não é aqui necessário o parecer da CNPD.

77. Ora, a CNPD chama a atenção para o facto de ser, precisamente, a utilização deste tipo de câmaras que tem revelado as maiores dificuldades no cumprimento dos requisitos regulamentares (hoje vigentes) que visam garantir a segurança do sistema de videovigilância e a integridade, confidencialidade e auditabilidade do

tratamento dos dados pessoais decorrente da sua utilização[2]. Por essa razão, deve a lei, para que não sobrem dúvidas, explicitar a necessidade neste tipo de procedimento de obtenção de parecer prévio da CNPD no n.º 1 do artigo 10.º, por referência expressa a tal consulta prévia ou por remissão para o artigo 5.º da Proposta de Lei.

78. De outro modo, e na falta de uma verificação prévia por quem tem conhecimentos especializados e experiência nesta matéria, com a agravante de em causa poder estar a utilização de aeronaves não tripuladas (*drones*), há um sério risco de não serem ponderadas no processo autorizativo eventuais insuficiências do sistema de videovigilância para ser apto a cumprir as finalidades visadas com a sua utilização ou aspetos do tratamento que impliquem a restrição ilícita da privacidade dos cidadãos.

(ii) Falta de elementos necessários à decisão de autorização

79. Sublinha-se ainda não se alcançar a seleção dos elementos que devem instruir o pedido de autorização da utilização de câmaras portáteis, constante do n.º 3 do artigo 10.º da Proposta. Na verdade, com exceção das normas constantes das alíneas *a)* e *c)* – muito embora o disposto na alínea *a)* tenha de ser aplicável com as devidas adaptações, porque este tipo de pedidos tem de ser acompanhado de uma específica fundamentação quando à adequação e necessidade da sua utilização – , não se alcança por que se exclui o procedimento de informação ao público, a identificação dos dados biométricos sujeitos a recolha e os mecanismos tendentes a assegurar o correto uso dos dados registados (cf. alíneas *f), h)* e *i)* do n.º 1 do artigo 6.º da Proposta).

80. Insiste-se: a utilização de câmaras portáteis, não apenas quanto à recolha das imagens e som, mas também quando às condições da sua transmissão e subsequente tratamento, exige uma especial atenção no que diz respeito à confidencialidade, integridade e auditabilidade do tratamento. Além de, se as câmaras portáteis estiverem acopladas a aeronaves não tripuladas, se justificarem especiais deveres de informação ao público. É, por isso, inexplicável e inadmissível a não remissão para os referidos elementos instrutórios, recomendando a CNPD que tal lacuna seja integrada, nos termos supra enunciados.

(iii) Ausência de regulação da utilização de *drones*

81. Finalmente, centra-se a atenção no n.º 2 do artigo 10.º da Proposta, que prevê a utilização de câmaras portáteis através de qualquer meio de portabilidade, com especial enfoque na utilização de aeronaves não tripuladas (*drones*).

---

[2] Cf. os pareceres da CNPD, disponíveis em: Parecer/2021/141, de 29 de outubro, Parecer/2021/51, de 27 de abril, Parecer/2020/139, de 19 de novembro, Parecer/2020/41, de 1 de abril, disponíveis em https://www.cnpd.pt/decisoes/historico-de-decisoes/?year=2021&type=4&ent= e https://www.cnpd.pt/decisoes/historico-de-decisoes/?year=2020&type=4&ent=

82. Não pode deixar de surpreender a forma simplificada, dir-se-ia mesmo simplista, com que vem prevista na Proposta de Lei a utilização de aeronaves não tripuladas. Como se a mera atestação legislativa da possibilidade genérica da sua utilização fosse suficiente para cumprir a função da lei de orientação das condutas de entidades públicas, e especificamente, das forças de segurança, e a função de previsibilidade que uma lei restritiva de direitos, liberdades e garantias sempre tem de garantir aos titulares destes direitos.

83. Não se fixam quaisquer condições ou limites específicos para a utilização de câmaras portáteis quando incorporadas em *drones*, como se fosse similar, sequer comparável, o impacto sobre a vida privada de uma câmara transportada por um agente que circula numa rua, ou transportada numa embarcação em alto mar, e uma câmara que sobrevoa a determinada altitude, e com nenhuma ou muito reduzida perceção de tal facto por parte dos transeuntes, as ruas de uma cidade, as praias, os jardins públicos e, porventura, os jardins e terraços privados. Aliás, com aptidão também para voar num plano nivelado com prédios, captando imagens do interior dos edifícios, que podem ser habitações.

84. E, no entanto, na Exposição de Motivos da proposta de lei pode ler-se a intenção de «[...] acomodar a utilização das câmaras incorporadas em sistemas de aeronaves não tripuladas [...] pelas forças e serviços de segurança, *na sua atividade diária*» (itálico nosso), o que revela bem que, a *ratio* desta proposta de lei é vulgarizar ou generalizar o uso de *drones* para vigiar os cidadãos, sem delimitar o seu uso a específicas finalidades e independentemente da sua efetiva adequação e necessidade, secundarizando o impacto nos direitos fundamentais decorrente da sua utilização.

85. Não se resiste a transcrever aqui o considerando 33 da Diretiva (UE) 2016/680, de 27 de abril, que a Lei n.º 59/2019, de 8 de agosto transpõe, onde se pode ler, quanto ao fundamento jurídico ou a medida legislativa nacional para que remeta a própria diretiva, que esses «[...] *deverão ser claros e precisos, e a sua aplicação deverá ser previsível para os particulares, como exigido pela jurisprudência do Tribunal de Justiça e pelo Tribunal Europeu dos Direitos do Homem. O direito dos Estados-Membros que rege o tratamento de dados pessoais no âmbito da presente diretiva deverá especificar, pelo menos, os objetivos, os dados pessoais a tratar, as finalidades do tratamento e os procedimentos destinados a preservar a integridade e a confidencialidade dos dados pessoais, bem como os procedimentos para a destruição dos mesmos, proporcionando assim garantias suficientes contra o risco de abusos e de arbitrariedade*». Como facilmente se depreende, este diploma, quanto à utilização de *drones*, não cumpre manifestamente este requisito de densificação legislativa e de previsibilidade, recordando-se que, nos termos da Constituição portuguesa (cf. artigo 18.º e alínea *b)* do n.º 1 do artigo 165.º da CRP), essas regras e garantias devem encontrar definição no plano legislativo e não no plano regulamentar.

86. A CNPD entende, por isso, imprescindível que neste diploma se regule a utilização de câmaras incorporadas ou acopladas a aeronaves não tripuladas em termos que garantam que, salvo autorização do juiz no âmbito de um processo criminal, não sejam captadas imagens e som do interior de edifícios, de varandas, terraços, jardins e quaisquer outros espaços do domínio privado. Quanto aos espaços públicos e de acesso público, se especifique a imprescindibilidade de garantir que a restrição aos direitos fundamentais, máxime do direito ao respeito pela vida privada e familiar, é adequada, necessária e não excessiva relativamente à finalidade prosseguida no caso concreto, especificando-se no diploma legal as específicas finalidades que podem justificar a sua utilização. Não se esqueça que o artigo 3.º, tal como está redigido, abarca finalidades de diferente relevância, pois ao lado da prevenção e repressão de ilícitos criminais se admite também a tutela de bens secundários, cuja agressão constitui um ilícito de mera ordenação social. Impõe-se, por isso, que a lei reflita a ponderação entre os bens jurídicos em tensão, só legitimando a ingerência na vida privada com a intensidade que os *drones* potenciam se os bens jurídicos ameaçados ou lesados merecerem a tutela reforçada da legislação penal.

87. A CNPD sublinha ainda ser essencial a imposição da adoção de formas adequadas de cumprimento do dever de informação ao público, conforme previsto no artigo 14.º da Lei n.º 59/2019, de 8 de agosto – a este ponto voltaremos infra, nos pontos 145 a 148.

88. Demais, é essencial que se definam as condições de recolha, transmissão e utilização das imagens e som captados, precisamente para que se previna o risco de interferência externa, de manipulação das imagens e som captados, garantindo-se assim a integridade, a confidencialidade e, especialmente, a auditabilidade do tratamento desses dados. A regulação destes aspetos do tratamento de dados em termos mais específicos e técnicos poderá ser feita no plano regulamentar, mas cabe à lei prever essa remissão ou delegação, embora reservando para si quais as salvaguardas aplicáveis para a defesa dos direitos, liberdades e garantias, o que no artigo 10.º da Proposta de Lei manifestamente não sucede.

89. De outro modo, a mera previsão genérica da utilização de câmaras portáteis em *drones*, no n.º 2 do artigo 10.º, sem se preverem condições que demonstrem a necessidade dessa utilização, nem medidas que revelem a ponderação e acautelem o impacto diferenciado e mais intenso do tratamento de dados na esfera jurídica dos cidadãos, implica uma restrição desproporcionada dos direitos fundamentais ao respeito pela vida privada e familiar e à proteção dos dados pessoais, em violação do n.º 2 do artigo 18.º da CRP.

c. A utilização de *bodycams*

90. Importa agora considerar a utilização de câmaras portáteis de uso individual, regulada no artigo 11.º da Proposta de Lei, *para efeitos de registo de intervenção individual de agente das forças de segurança em ação policial* (cf. n.º 1).

91. A utilização de câmara de vídeo por cada agente das forças e serviços de segurança coloca o desafio específico de conciliar a tutela da privacidade dos próprios agentes e de todos os cidadãos com que se vão cruzando no exercício de «ação policial» com a tutela do interesse que a sua utilização visa acautelar. Sendo certo que tal interesse não vem explicitado, parecendo apresentar-se o registo da intervenção individual do agente como um fim em si mesmo. Na realidade, esta previsão terá na sua base casos recentes em que as conduta de agentes foram gravadas por cidadãos através dos seus telemóveis e *smartphones* e divulgadas em redes sociais, o que gera a convicção de que os agentes devem estar dotados de ferramentas similares que lhes permita demonstrar a sua versão do mesmo evento.

92. Compreendendo-se esse interesse – que corresponderá à recolha de prova relativa a condutas dos agentes e dos cidadãos que com estes interajam – não deixa, porém, de ser necessário acautelar os direitos e liberdades dos cidadãos e, desde logo, garantir que o regime definido no artigo 11.º seja apto a atingir o objetivo visado. Vejamos.

93. A solução consagrada na Proposta de Lei faz depender a utilização da câmara de autorização do respetivo dirigente máximo, disso sendo prestada informação ao membro do Governo que tutela a força de segurança (cf. n.º 1 do artigo 11.º da Proposta). Esta primeira disposição não é, na perspetiva da CNPD, clara quanto ao objeto e âmbito da autorização: se em causa está a autorização da colocação da câmara no uniforme ou equipamento do agente sempre que o mesmo vai entrar em ação policial (e subsequente informação do membro do Governo), ou se se tem em vista a primeira vez que a um agente é atribuída uma câmara para tais efeitos. A CNPD recomenda, por isso, a sua clarificação.

94. Quanto ao pressuposto que fundamenta a possibilidade de ativação da câmara, e subsequentes captação e gravação de imagens e som, o n.º 3 do artigo 11.º da Proposta indica ser «*em caso de intervenção de elemento das forças de segurança*», pressuposto que vem em seguida exemplificado com várias circunstâncias, caracterizadas através de conceitos imprecisos. Não explicitando o preceito quem toma a decisão de ativar a câmara, parece ser o agente das forças de segurança e, portanto, a este a lei está a atribuir um poder discricionário de ligar a câmara quando se verifique uma daquelas circunstâncias (que são, repete-se, meramente exemplificativas).

95. Ora, se se compreende que este poder de decisão discricionária, assim delimitado, quanto à ativação da câmara vem limitar o impacto que uma câmara a gravar imagem e som durante todo o turno do agente teria sobre a vida privada do próprio e de todos os cidadãos que com ele se pudessem cruzar, a verdade é que a solução encontrada não se afigura idónea a cumprir a finalidade visada.

96. Com efeito, parece falhar aqui a primeira vertente do princípio da proporcionalidade: esta medida, assim delimitada, deixa ao agente a faculdade de ativar ou não a câmara, mesmo quando esteja «em intervenção», e deixa-lhe o poder de concluir se é uma situação que legitima a sua ativação. Por outras palavras, a solução aqui encontrada não acautela o risco ou a probabilidade de o agente não querer que seja captada e gravada parte ou a totalidade da sua ação, sendo de duvidosa utilidade para efeito de prova da sua intervenção. Desde logo, não se determina se as imagens e som são transmitidos em tempo real, ou se ficam gravados no equipamento na posse do agente e, portanto, se há risco de manipulação ou eliminação das gravações. Na verdade, nos termos em que vem pensada, a utilização destas câmaras não parece ser apta ou idónea a cumprir a finalidade, declarada no n.º 1, de «registo de intervenção individual de agente das forças de segurança em ação policial».

97. Além destes dois aspetos, o artigo preocupa-se apenas com a garantia de transparência deste tratamento de dados pessoais – fazendo referência a uma sinalética que indique a finalidade da sua utilização (que, reitera-se, ficou explicada na lei como «registo de intervenção individual de agente das forças de segurança em ação policial») – e a um aviso verbal, presume-se, de que a gravação vai ser iniciada «sempre que a natureza do serviço e as circunstâncias o permitam» (cf. n.º 2 e n.º 3, *in fine*).

98. Todavia, o artigo para neste ponto, nada mais regulando; opta-se por remeter para portaria governamental a definição das «características e normas de utilização das câmaras [...], bem como a forma de transmissão, armazenamento e acesso aos dados recolhidos».

99. E aqui reside a segunda principal preocupação da CNPD. A acrescer à falta de adequação do tratamento dos dados para a finalidade visada, se esta fosse ultrapassável, ainda haveria a necessidade de prever regras relativas ao momento em que deve cessar a captação e gravação de imagens e som, bem como à hipótese de ser emitida uma ordem superior de gravação da intervenção, e que previnam os riscos de eliminação, manipulação ou divulgação do material gravado. Regras que, na perspetiva da CNPD, devem ser definidas em sede legislativa, precisamente porque servem a garantia dos direitos fundamentais dos cidadãos.

100. De outra forma, teremos a previsão de mais um tratamento de dados pessoais que implica a restrição de direitos fundamentais dos cidadãos, sem que aquela seja acompanhada, ao menos, da imposição de garantias adequadas a tutelar os direitos e interesses de todos os cidadãos, o que compreende também os próprios agentes das forças de segurança.

101. Em suma, por não se revelar apto a prosseguir a finalidade visada, a previsão legal da utilização de câmaras de uso individual, tal como se encontra redigida no artigo 11.º, viola a primeira manifestação do princípio da proporcionalidade, em contradição com o disposto no n.º 2 do artigo 18.º da CRP.

d. Outros regimes especiais

102. Quanto aos sistemas de vigilância da navegação marítima e fluvial, regulados no artigo 14.º da Proposta, chama-se a atenção para a necessidade de a instalação dos mesmos ter de acautelar que não sejam captadas imagens de propriedades privadas, devendo também prever-se a adoção de medidas que, assegurando a finalidade visada, eliminem ou reduzam ao mínimo indispensável o impacto sobre a privacidade das pessoas em espaços públicos em que as pessoas estão mais expostas, como sucede no contexto da utilização de praias marítimas e fluviais.

103. A CNPD recomenda ainda que seja especificada uma nota quanto à necessidade de, em todos os procedimentos especiais aqui regulados, cumprir o procedimento previsto no artigo 5.º da Proposta de Lei, o qual inclui a consulta prévia da CNPD. Esta observação prende-se com o facto de no artigo 15.º da Proposta, relativo aos sistemas de vigilância e deteção de incêndios, quando se impõe a consulta à Autoridade Nacional de Emergência e Proteção Civil, se referir expressamente o parecer da CNPD. Mas ao explicitar-se aí a necessidade da consulta da CNPD (redação que já se encontra na Lei n.º 1/2005) e não se fazer o mesmo nos outros artigos onde (inovatoriamente em relação à Lei n.º 1/2005) se regulam especialmente outros sistemas de vigilância (12.º e 14.º), permite-se a interpretação de que estaria nestes casos dispensado esse procedimento consultivo.

104. Não se afigurando, *prima facie*, ser essa a *ratio legis*, nem se vislumbrando um fundamento objetivo e razoável para o afastamento da instrução do procedimento com um parecer da autoridade administrativa que tem competências de supervisão prévia (hoje, essencialmente consultiva) e sucessiva em matéria de proteção de dados pessoais, a CNPD toma a liberdade de insistir na necessidade de explicitação desse dever de consulta prévia.

vi. Um novo regime especial de captação de imagens

105. No âmbito do capítulo IV, intitulado *Acesso a outros sistemas de videovigilância*, surge o artigo 17.º da Proposta, sob a epígrafe *Captação de imagens sem gravação*, a prever a possibilidade de captação de imagens, com recurso a câmaras fixas ou portáteis, exclusivamente para visualização em tempo real.

106. Assinala-se, em primeiro lugar, que esta norma, tal como se encontra redigida, não corresponde ao *acesso* a sistemas de videovigilância, mas antes a uma específica utilização de tais sistemas, pelo que se recomenda a reponderação da sua inserção sistemática neste capítulo, ou a alteração da denominação deste.

107. Mais importante é, contudo, o regime substantivo que aqui se estabelece. Admite-se a utilização de câmaras fixas ou portáteis para visualização de imagens desde que em causa estejam as finalidades previstas nas alíneas *c), e), f)* e *l)* do artigo 3.º, as quais parecem respeitar, grosso modo, a intervenções operacionais das forças de segurança.

108. Ora, em primeiro lugar, quanto à *utilização de câmaras fixas* neste contexto, não se alcança qual seja a sua autonomia relativamente aos regimes de instalação e utilização de câmaras fixas regulados nos artigos 5.º a 9.º da Proposta. Na verdade, se as câmaras já estão instaladas, então é sempre possível a sua utilização apenas para visualização. Se, diferentemente, aqui se tem em vista o acesso a sistemas de videovigilância de terceiros, então a norma tem de o dizer expressamente, por razões de certeza jurídica. Mas aí suscita-se uma outra questão – que em seguida se analisará (cf. infra, pontos 116 a 119) – e que respeita ao acesso remoto a tais sistemas.

109. No que diz respeito à utilização de *câmaras portáteis* para visualização, a CNPD não alcança por que é que esta utilização não vem regulada no artigo 10.º da Proposta, ou em todo o caso no capítulo III relativo a regimes especiais, por aqui se prever um procedimento simplificado, dependente unicamente da autorização do dirigente máximo das forças e serviços de segurança.

110. Recorda-se que a visualização em tempo real pode incluir (e dir-se-ia incluir aqui, para ter alguma utilidade) a transmissão das imagens para visualização num centro de comando e controlo, o que implica a necessidade de adotar medidas de segurança quanto ao processo de transmissão, o qual, em si mesmo, já implica um tratamento de dados. E, como em seguida, no n.º 2 do artigo 17.º, se prevê a possibilidade de gravação, então é imprescindível a imposição legal de medidas especiais que garantam a segurança, confidencialidade e integridade do tratamento, bem como a sua auditabilidade, como sucede em qualquer outro tratamento de dados pessoais decorrente da utilização de câmaras portáteis.

111. Mas repare-se que o disposto no artigo 17.º abrange também a utilização de *drones* (ou aeronaves não tripuladas), o que significa a possibilidade de, apenas por determinação do dirigente máximo das forças e serviços de segurança, se proceder à utilização de câmaras portáteis incorporadas em *drones*. E esta possibilidade vem assim enunciada, para ser concretizada num procedimento decisório simplificado, sem qualquer densificação de condições ou limites materiais para a tomada de tal decisão

112. A CNPD insiste que este tipo de normas, meramente enunciativas da possibilidade da utilização de equipamentos com um enorme potencial intrusivo na vida privada e familiar, sem definição de quaisquer

garantias dos direitos fundamentais dos cidadãos, não cumpre as exigências mais básicas do Estado de Direito, suportando-se exclusivamente na afirmação de um interesse público (ou privado) como bem maior, sem que se obrigue previamente a um rigoroso processo de ponderação da adequação, necessidade e proporcionalidade (no sentido de não excessividade) da utilização daquele tipo de equipamentos. E sem que se obrigue a adoção de medidas que mitiguem o evidente impacto que essa utilização tem na vida privada dos cidadãos. Remete-se, por isso, para as recomendações e conclusões deixadas supra, nos pontos 86 a 89, face à evidente inconstitucionalidade de uma norma legal com este alcance restritivo de direitos, liberdades e garantias, por não se delimitar a restrição e, portanto, ela se apresentar, assim, sem mais pressupostos, como desnecessária ou, pelo menos, excessiva, em clara violação do n.º 2 do artigo 18.º da CRP.

vii. Acesso remoto a sistemas de videovigilância de entidades públicas ou privadas

113. No referido capítulo IV, regula-se, no artigo 16.º da Proposta, o acesso a sistemas de videovigilância de qualquer entidade pública ou privada, instalados em locais públicos ou privados de acesso público, para os fins previstos no artigo 3.º da Proposta.

114. A este propósito, a CNPD faz duas observações. A primeira, para assinalar que, de acordo com a Exposição de Motivos, através da Proposta «clarificam-se os regimes especiais e densificam-se os procedimentos relativos à utilização, por parte das forças e serviços de segurança, de sistemas de videovigilância criados pelos municípios, bem como o acesso aos sistemas privados de videovigilância instalados em locais públicos ou privados de acesso ao público», quando em rigor o disposto no artigo 16.º não clarifica nem densifica o acesso que já estava previsto no n.º 7 do artigo 31.º da Lei n.º 34/2013, de 16 de maio, alterado pela Lei n.º 46/2019, de 8 de julho (que fixa o regime jurídico da segurança privada). E que, para os sistemas de videovigilância nos espaços de restauração e bebidas com espaços ou salas destinadas a dança, o n.º 5 do artigo 5.º do Decreto-Lei n.º 135/2014, de 8 de setembro, na redação dada pela Lei n.º 35/2019, de 24 de maio, já prevê o visionamento das imagens em tempo real no centro de comando e controlo.

115. Não se vislumbra, pois, que densificação aqui seja feita, para além do alargamento desta possibilidade a todos os sistemas de videovigilância de qualquer entidade pública ou privada, instalados em locais públicos ou privados de acesso público.

116. A CNPD já se pronunciou sobre esta matéria a propósito das alterações legais de 2019[3], mantendo a necessidade de se estabelecer que a possibilidade de acesso remoto deve ser contextualizada, através da

[3] Cf. Parecer 52/2018 e Parecer 53/2018, ambos de 13 de novembro, acessíveis em https://www.cnpd.pt/decisoes/historico-de-decisoes/?year=2018&type=4&ent=

demonstração da sua adequação e necessidade a uma concreta finalidade – o que se afigura existir, *prima facie*, em relação aos estabelecimentos onde, nos termos legais, deve existir um sistema de videovigilância (*v.g.*, ourivesarias, bancos) – e chamando a atenção para os riscos que do acesso remoto podem resultar para os sistemas de videovigilância das entidades públicas e privadas, quando o acesso remoto não é efetuado através de um canal seguro. Os riscos não são apenas relativos à segurança de tais sistemas, por eventualmente potenciar o acesso indevido, a eliminação e a manipulação de imagens por terceiros, como também, em consequência, os relativos à privacidade que decorrerão da divulgação e manipulação das imagens por terceiros.

117. Acresce que, além de não se ver que desta norma resulte, sem mais, um dever de todas estas entidades criarem um canal seguro – e, portanto, tal dever recairia sobre as forças de segurança –, não se vislumbra que canal possa ser criado que garanta o acesso seguro a todos os sistemas de videovigilância aqui abrangidos.

118. De resto, fica por esclarecer em que nível – centralizado a nível nacional, ou antes delimitado a nível local – se processa o acesso a tais sistemas.

119. A CNPD considera, assim, que a previsão de possibilidade de acesso remoto tem de ser reponderada e, a manter-se *a final*, tem de ser acompanhada da imposição de adoção de medidas que mitiguem os riscos decorrentes daí decorrentes.

viii. Utilização de tecnologias de Inteligência Artificial e tratamento de dados biométricos

120. O capítulo VI da Proposta de Lei, sob o título *Tratamento de dados,* traz importantes novidades ao regime da videovigilância no espaço público e também no espaço privado de acesso público, na medida em que também este é abrangido pelo âmbito de aplicação da Proposta de Lei.

a. Inteligência artificial

121. Na verdade, admite-se no n.º 1 do artigo 18.º que a *visualização e o tratamento de dados podem ter subjacente um sistema de gestão analítica de dados captados, por aplicação de critérios técnicos de acordo com os fins a que os sistemas se destinam.*

122. Mais uma vez, a previsão genérica de utilização de tecnologia que implica um impacto na esfera jurídico-fundamental dos cidadãos de diferente intensidade, consoante o tipo de ferramenta de analítica de dados a utilizar, se revela manifestamente insuficiente para que a lei cumpra a sua função de orientação das forças e serviços de segurança quanto a essa utilização e, objetivamente, insuficiente para permitir aos cidadãos compreender em que condições vai ser utilizado e que impacto pode ter nos seus direitos fundamentais. Desde logo, sem que se perceba se essas ferramentas podem ser utilizadas para qualquer das finalidades previstas no artigo 3.º da Proposta, portanto, também para as finalidades de tutela de interesses de mera ordenação social.

b. Previsão encoberta de tecnologia de reconhecimento facial

123. E se a esta mera previsão genérica se juntar a permissão, logo no número seguinte do mesmo artigo 18.º, do tratamento de dados biométricos, então temos uma norma legislativa que, desta forma subtil e encoberta, dá abertura à incorporação de tecnologia de reconhecimento facial nos sistemas de videovigilância em espaço público. Mais, como acima se referiu, atendendo ao âmbito de aplicação da Proposta de Lei, definida no seu artigo 2.º, tal incorporação será possível também nos sistemas de videovigilância em espaço privado de acesso ao público, se no n.º 1 do artigo 18.º não se restringir o seu âmbito de aplicação.

124. A previsão encoberta da utilização de tecnologia de reconhecimento facial vem, mais adiante no artigo, confirmada. Na verdade, o n.º 4 do artigo 18.º não deixa dúvidas quanto ao que se pretende referir com a captação de dados biométricos: não se trata apenas da captação da imagem da pessoa, e da análise de dados biométricos (*v.g.*, a forma de andar), mas da criação de um *template* biométrico do seu rosto.

125. A circunstância de o legislador nacional, na presente Proposta, incorporar no mesmo artigo a permissão de utilização de tecnologia de analítica de dados e a permissão de tratamento de dados biométricos, sem afirmar expressamente a permissão de utilização de tecnologia de reconhecimento facial, não deixa de surpreender, quando num Estado de Direito democrático as restrições aos direitos, liberdades e garantias devem ser determinadas por lei de forma clara e taxativa.

126. Desconhece a CNPD se o legislador nacional está ciente das consequências reais da utilização deste tipo de tecnologia em sistemas de videovigilância no espaço público e no espaço privado de acesso ao público. Trata-se, na realidade, de dar luz verde à vigilância em massa pelas forças e serviços de segurança, negando qualquer dimensão de privacidade que ainda pudesse restar no espaço público (e no espaço privado aberto ao público). Ela permite o rastreamento dos cidadãos potenciado pela possibilidade de relacionamento das informações disponíveis nos sistemas de videovigilância dos estabelecimentos públicos e privados e demais espaços privados abertos ao público, a que se soma a utilização na atividade diária das forças e serviços de segurança das câmaras portáteis também por via do recurso a *drones*.

127. Sendo evidente o impacto que tal controlo pode ter sobre qualquer sociedade democrática, pela facilidade com que esta ferramenta é utilizável como meio de repressão das liberdades de expressão, de manifestação e de reunião, como exemplos recentes noutros pontos do mundo o têm demonstrado.

128. Não é preciso, seguramente, recordar aqui a jurisprudência do Tribunal Constitucional e a jurisprudência do Tribunal Europeu dos Direitos Humanos, ou mesmo do Tribunal de Justiça da União Europeia, todas afirmando um direito ao respeito pela vida privada no espaço público. Jurisprudência que vem insistindo na imprescindibilidade de, num Estado de Direito democrático, a lei delimitar com precisão as restrições aos direitos

e liberdades dos cidadãos, quando as mesmas se revelem adequadas a prosseguir determinados valores públicos fundamentais, sob pena de se ter tais restrições como desproporcionais ou mesmo como afetando o conteúdo essencial desses direitos.

129. Ora, o artigo 18.º da Proposta é absolutamente vazio de condições e critérios de utilização das tecnologias de analítica de dados e, especialmente, do reconhecimento facial. Limita-se a remeter no n.º 1 para a *aplicação de critérios técnicos de acordo com os fins a que os sistemas se destinam*. Nem sequer especificando quem define tais critérios.

130. Oportuno é ainda recordar que a *Proposta de Resolução do Parlamento Europeu sobre a inteligência artificial no Direito penal e a sua utilização pelas autoridades policiais e judiciárias em casos penais* «[d]estaca que a utilização de dados biométricos está mais amplamente relacionada com o princípio do direito à dignidade humana, que constitui a base de todos os direitos fundamentais garantidos pela Carta; Considera que a utilização e a recolha de quaisquer dados biométricos para fins de identificação à distância, por exemplo, através de reconhecimento facial em espaços públicos, bem como em cancelas de controlo automatizado de fronteiras utilizadas em controlo fronteiriços nos aeroportos, podem acarretar riscos específicos para os direitos fundamentais, cujas implicações podem variar consideravelmente em função da finalidade, do contexto e do âmbito da utilização; salienta ainda a validade científica contestada da tecnologia de reconhecimento, designadamente de câmaras que detetam movimentos oculares e alterações na dimensão da pupila, num contexto policial; entende que o uso da identificação biométrica nos contextos policial e judicial deve ser sempre considerada de «alto risco» e, por conseguinte, sujeita a requisitos adicionais, de acordo com as recomendações do Grupo de Peritos de Alto Nível sobre IA da Comissão»[4].

131. E ainda que, no final da Exposição de Motivos da Proposta de Resolução, se lê: «Por último, *o relator solicita uma moratória para a implantação de sistemas de reconhecimento facial para fins policiais*. O estado de avanço destas tecnologias e o seu importante impacto nos direitos fundamentais exigem um debate profundo e aberto na sociedade, a fim de examinar as diferentes questões que se colocam e a justificação para a sua implantação» (itálico nosso), o que é bem sinal de que a opção de utilização de desta tecnologia no espaço público para fins policiais não está ainda suficientemente amadurecida.

132. Demais, abundam os estudos que revelam que a utilização de tecnologia de reconhecimento facial nos sistemas de videovigilância gera elevadas taxas de falsos positivos na identificação das pessoas. Em especial,

[4] Cf. § 30 da Proposta de Resolução, acessível em https://www.europarl.europa.eu/doceo/document/A-9-2021-0232_PT.html#title6

quando as imagens são de pessoas com determinada origem étnica ou racial, em especial de mulheres[5] [6]. Ora, em face de tais taxas de erro e em especial com a relevância que assume a origem étnica ou racial na sua promoção, o risco de discriminação é demasiado para que possa ser assim assumido de forma ligeira na nossa legislação.

c. Incongruências técnicas e jurídicas da redação do artigo 18.º

133. Sem prejuízo de tudo o que vem de se dizer, analisar-se-á agora o regime previsto no artigo 18.º, para sublinhar as suas diferentes incongruências e lacunas.

134. Desde logo, opta-se no n.º 1 do artigo 18.º por diferenciar a *visualização* e o *tratamento* de dados, para efeitos de aplicação de tecnologia de analítica de dados, quando a própria transmissão dos dados para efeito de visualização e ulterior análise, no servidor central, sempre implica uma operação de tratamento de dados; pelo que, logo por aqui, perderia sentido a referência ao processo de visualização. Mas a incongruência adensa-se quando se compreende que a aplicação daquela tecnologia não pode ocorrer num simples processo de mera visualização.

135. Depois, o n.º 2 e o n.º 3 do artigo 18.º são disposições de difícil interpretação e articulação. Não se podem *captar* dados biométricos, no sentido que lhe está a ser dado no n.º 4 do mesmo artigo – portanto, para efeito ou através da criação de um *template* –, sem que tais dados sejam objeto do necessário *tratamento* para a criação do *template* biométrico, pelo que falar-se em captação no n.º 2 e tratamento desses mesmos dados no n.º 3 é completamente destituído de lógica e revela pouco rigor técnico.

136. Portanto, o que parece querer prever-se é o tratamento de dados biométricos de todos aqueles que se encontrem ou circulem no espaço público ou em espaço aberto ao público – numa lógica de recolha em massa

---

[5] Cf. Leslie, D. (2020). Understanding bias in facial recognition technologies: an explainer. The Alan Turing Institute, in https://doi.org/10.5281/zenodo.4050457, e Joy Buolamwini / Timnit Gebru, Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, Proceedings of Machine Learning Research 81:1–15, 2018, in http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

[6] Cf, Peter N. Schuetz, Fly in the Face of Bias: Algorithmic Bias in Law Enforcement's Facial Recognition Technology and the Need for an Adaptive Legal Framework, 39(1) LAW & INEQ. (2021), acessível em https://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=1656&context=lawineq, e especialmente a referência que aí se faz a um estudo realizado em julho de 2018 pela American Civil Liberties Union (ACLU), no âmbito do qual fez correr o *software Recognition* da Amazon, anunciado como oferecendo "highly accurate facial analysis, face comparison, and face search capabilities", sobre fotografias de membros do 115.º Congresso dos Estados Unidos da América e comparou-a com uma base de dados pública de 25 000 fotografias de presos; embora nenhum dos congressistas estivesse entre este universo de presos, o *software* apresentou o resultado de 28 "matches", tendo-se verificado depois que o erro respeita a um número desproporcionado de congressistas afro-americanos.

de dados biométricos. Mas a norma não define aquilo que, neste quadro, seria crucial: se os dados biométricos vão constar de uma base de dados centralizada e quem será o responsável por tal sistema de informação.

137. Mais, neste pressuposto, não se percebe se no n.º 3 se pretende limitar o acesso a essa base de dados para a finalidade de prevenção de atos terroristas, caso em que o acesso depende de uma autorização judicial, que se presume, embora o legislador não o diga, ocorrer num específico processo judicial, ou se, com o mesmo n.º 3, se pretende fazer depender o acesso a tais dados biométricos de uma autorização judicial apenas quando em causa esteja a finalidade de prevenção de atos terroristas. O que significaria que, para as demais finalidades do artigo 3.º ainda seria possível aceder à tal base de dados biométrica – muitas das quais, como se referiu, nem sequer respeitam à prevenção e repressão criminal.

138. Finalmente, este artigo termina com uma disposição que, ao limitar a realização de avaliações de impacto aos casos de utilização de tecnologias de inteligência artificial, restringe o âmbito da obrigação decorrente do Direito da União Europeia de realizar uma avaliação de impacto. Tal obrigação está prevista no RGPD (cf. alínea *c)* do n.º 3 do artigo 35.º) quando em causa estejam os sistemas de videovigilância regulados nos artigos 12.º, 14.º e 15.º da Proposta de Lei, e, quanto à utilização dos sistemas para as demais finalidades previstas no artigo 3.º da Proposta, também no artigo 27.º da Diretiva (UE) 2016/680, que prevê o dever de os Estados-Membros vincularem os responsáveis pelo tratamento à realização da avaliação de impacto sobre a proteção de dados pessoais, lido à luz do considerando 51, *in fine* (onde se considera ser sempre de elevado risco para os direitos e liberdades o tratamento que incida sobre uma grande quantidade de dados pessoais e afetar um grande número de titulares de dados).

139. Nesse sentido, deve ser eliminado o n.º 5 do artigo 18.º da Proposta, por estar a restringir uma obrigação imposta pelo RGPD e pela citada Diretiva.

140. Em suma, o artigo 18.º da Proposta prevê um sistema de vigilância em massa por recurso genérico a tecnologias de analítica de dados e de reconhecimento facial, o que representa uma restrição de direitos fundamentais dos cidadãos, sem cumprir os ditames do Estado de Direito, sequer quanto à imprescindível clareza e transparência quanto à previsão dessas restrições, e sem prever quaisquer garantias daqueles direitos, e por isso se revela violadora das exigências fixadas nos n.ºs 2 e 3 do artigo 18.º da CRP, sendo suscetível de afetar o conteúdo essencial do direito ao respeito pela vida privada e violando manifestamente o princípio da proporcionalidade.

ix. Responsabilidade pelo tratamento de dados pessoais e as relações de subcontratação

141. No que diz respeito ao artigo 19.º da Proposta de Lei, a CNPD gostaria de destacar a importância de que se preveja neste artigo que eventuais subcontratações de serviços de instalação e de manutenção dos sistemas de videovigilância ou de fornecimento de *software* a incorporar nos mesmos tem de obedecer ao estabelecido no artigo 23.º da Lei n.º 59/2019, de 8 de agosto, e no artigo 28.º do RGPD (quanto aos sistemas previstos nos artigos 12.º, 14.º e 15.º da Proposta).

142. E insiste-se neste ponto porque, na sua atividade de acompanhamento dos tratamentos de dados pessoais realizados pelas forças de segurança no contexto da utilização de sistemas de videovigilância, a CNPD tem constatado a falta de meios e de formação adequada das forças de segurança para determinar com precisão as operações a realizar e controlar a sua execução (cf. supra, pontos 14 a 30).

x. Procedimentos relativos à gravação

143. Em relação aos artigos 20.º e 21.º da Proposta, destaca-se ser conveniente clarificar aquela que parece ser a opção legislativa de prever que as imagens extraídas para envio para o Ministério Público devem ser conservadas para além do prazo de eliminação previsto no n.º 1 do artigo 21.º. Neste último caso, deve determinar-se qual o prazo da sua eliminação e, se esse não for um prazo certo, prever-se um procedimento – a cargo do Ministério Público – de comunicação ao responsável pelo tratamento do momento a partir do qual deve proceder-se à sua eliminação.

144. Ainda quanto ao artigo 21.º, recomenda-se a correção da redação do n.º 4, por não ser adequada a expressão o «código [...] fica a cargo [...]». Assim, sugere-se a sua substituição pela indicação de que o código ou chave de cifragem deve ser do conhecimento exclusivo do responsável pelo tratamento dos dados.

xi. Falta de transparência na utilização de câmaras portáteis, incluindo em *drones*

145. Não pode deixar de se olhar com preocupação para o capítulo VII, já que os artigos 24.º e 25.º dizem apenas respeito à prestação de informação relativamente à *instalação de câmaras fixas*, tendo-se optado por uma total ausência de divulgação da utilização de câmaras portáteis.

146. A CNPD sublinha que o artigo 13.º da Diretiva 2016/680 (e o artigo 14.º da Lei n.º 59/2019, de 8 de agosto) atribui aos titulares de dados o direito de informação sobre o tratamento de dados pessoais, tendo a CNPD dúvidas que todos os tratamentos de dados pessoais realizados com recurso a câmaras portáteis estejam abrangidos pelas exceções naquele previstas.

147. A CNPD recomenda, por isso, que se pondere a extensão do disposto nos artigos 24.º e 25.º da Proposta às câmaras portáteis, sobretudo quando em causa esteja a sua utilização em áreas ou por causa de eventos bem delimitados, e especialmente quando estejam incorporadas em aeronaves não tripuladas (*drones*), onde as exigências de publicitação se colocam com maior intensidade, porque os cidadãos delas podem não se aperceber.

148. Mais recomenda que o artigo 24.º seja atualizado em face do estatuído no n.º 2 do artigo 13.º da citada Diretiva – e quanto aos tratamentos realizados no contexto dos sistemas previstos nos artigos 12.º, 14.º e 15.º da Proposta, em face do estabelecido no artigo 13.º do RGPD –, sob pena de a lei nacional estar em desconformidade com tais regimes. Eventualmente com definição de outros instrumentos para divulgação destas informações acrescidas, como por exemplo, no sítio da Internet das forças e serviços de segurança.

xii. A restrição dos poderes de supervisão prévia e sucessiva da CNPD

149. Finalmente, além das já acima assinaladas restrições decorrentes da eliminação da intervenção da CNPD em sede de consulta prévia nos procedimentos excecionais do artigo 9.º da Proposta e dos procedimentos especiais relativos à utilização de câmaras portáteis (artigos 10.º e 17.º da Proposta), também quando incorporadas em *drones*, importa aqui destacar duas aparentes restrições às competências da CNPD decorrentes do disposto no n.º 2 do artigo 23.º e do n.º 2 do artigo 26.º da Proposta.

150. O n.º 2 do artigo 23.º atribui à Inspeção-Geral da Administração Interna (IGAI) a competência para a emissão de recomendações que visem a melhoria dos procedimentos de recolha e tratamento de dados pessoais, através dos sistemas de videovigilância.

151. Nada tendo a CNPD a opor a que a IGAI emita recomendações sobre esta matéria, não deixa porém de assinalar que, tanto por força do artigo 57.º, n.º 1, alínea *d)*, do RGPD, quanto aos tratamentos de dados pessoais regulados na Proposta que a ele estão sujeitos, como por força do artigo 46.º, n.º 1, alínea *d)*, da Diretiva (UE) 2016/680, que a Lei n.º 59/2019, de 8 de agosto, transpôs a (cf. artigo 44.º), cabe à CNPD dar orientação aos responsáveis pelos tratamentos sobre as suas obrigações, e tal função não pode ser beliscada pelo legislador português enquanto a CNPD for considera pela lei nacional a autoridade nacional de proteção de dados também nesta área de atividade pública.

152. Assim, a CNPD sugere que se acrescente ao disposto no n.º 2 do artigo 23.º a ressalva *sem prejuízo das atribuições e competências da CNPD*.

153. Também a redação do n.º 2 do artigo 26.º da Proposta, quando impõe que *«[a] fiscalização exerce-se através de verificações periódicas dos sistemas de videovigilância e tratamento de dados recolhidos, por amostragem»*,

parece estar a condicionar a atividade inspetiva da CNPD em termos que não se coadunam totalmente com o espaço discricionário reconhecido pelo RGPD e pela citada Diretiva à autoridade nacional de controlo quanto à sua função inspetiva. Ainda que a intenção legislativa possa não ter sido essa, a imposição de que a fiscalização se faça por amostragem limita a competência inspetiva desta, precludindo uma eventual fiscalização exaustiva dos sistemas de videovigilância das forças e serviços de segurança.

154. A este propósito acrescenta-se dever ser corrigido o n.º 4 do artigo 26.º, quando faz referência ao dever de a CNPD ordenar o «cancelamento» de dados, porquanto o termo adequado será *eliminação* ou *apagamento* dos dados.

III. Conclusão

155. Com os fundamentos acima expostos, a CNPD entende que a Proposta de Lei, no conjunto das suas disposições, introduz um regime jurídico muito restritivo dos direitos fundamentais dos cidadãos, em especial dos direitos ao respeito pela vida privada e familiar e ao direito à proteção de dados pessoais, suscetível de afetar o conteúdo essencial do direito ao respeito pela vida privada, ao permitir a vigilância em massa no espaço público e nos espaços privados de acesso ao público.

156. Os termos amplos e imprecisos com que vem prevista a utilização, pelas forças e serviços de segurança, de sistemas de vigilância através de câmaras fixas e câmaras portáteis – estas últimas podendo estar incorporadas em aeronaves não tripuladas (*drones*) e nos equipamentos dos agentes (*bodycams*) –, indefinidamente para qualquer das finalidades admitidas na Proposta, com a possibilidade generalizada de utilização de tecnologias de inteligência artificial e de reconhecimento facial, não cumpre as exigências mínimas num Estado de Direito democrático para a restrição legislativa de direitos fundamentais.

157. O que perpassa ao longo do diploma é a opção pelo aligeiramento do regime da videovigilância para fins policiais, quer no plano procedimental, quer no plano substancial, para facilitar a sua utilização independentemente de uma efetiva e circunstanciada avaliação da sua adequação e necessidade à garantia de segurança pública ou de salvaguarda de bens especialmente merecedores de proteção. A *ratio* subjacente é a de que não é necessária a verificação de um risco ou perigo especial para tais bens para justificar a ingerência, num elevado grau (em especial quando combinado com certas tecnologias também aqui genericamente admitidas), nos direitos, liberdades e garantias, bastando a alegação de uma suposta sensação de insegurança.

158. A utilização de equipamentos e tecnologias potenciadores do impacto da utilização de câmaras de vídeo não vem prevista para específicas finalidades, parecendo ser indiferente para o legislador nacional se aqueles são usados para prevenir ou reprimir o crime ou para prevenir ou reprimir uma qualquer perturbação menor da

ordem pública. É o que se verifica quanto aos *drones*, às *bodycams* e às tecnologias de analítica de dados ou de reconhecimento facial.

159. Os procedimentos excecionais e especiais proliferam, deixando às próprias forças e serviços de segurança (*rectius*, ao seu dirigente máximo) a decisão de utilizar câmaras portáteis (também com *drones*) sem qualquer controlo prévio independente. E sem um efetivo controlo independente ulterior.

160. Basta enumerar aqui a:

i. ausência de definição, no plano legal, das condições e dos limites da utilização dos sistemas de videovigilância, em especial de câmaras portáteis, em relação às quais se preveem procedimentos decisórios simplificados e amplamente discricionários;

ii. a ausência de fixação dos critérios de aplicação das tecnologias de inteligência artificial, e especificamente relativamente aos dados biométricos;

iii. a opacidade da previsão legal de utilização de tecnologia de reconhecimento facial no espaço público e também nos sistemas privados de videovigilância que incidam sobre o espaço privado de acesso ao público;

iv. a falta de transparência quanto à utilização de câmaras portáteis, em especial quando acopladas a *drones*, ao limitar-se o dever de publicitação à instalação de câmaras fixas;

v. o prazo de 5 anos de duração das autorizações, que dispensa assim uma avaliação atualizada da aptidão e da necessidade da utilização das câmaras de videovigilância;

para se compreender que este diploma não faz depender a utilização dos sistemas de videovigilância de um juízo concretamente circunstanciado de adequação e necessidade quanto à finalidade visada, nem consegue cumprir a função de orientar as forças e serviços de segurança quanto à sua utilização, não prevenindo a possibilidade do seu uso arbitrário, tampouco cumprindo a função de previsibilidade quanto aos tratamentos de dados pessoais e consequências prováveis para os direitos fundamentais dos cidadãos.

161. Deste modo, e em especial, a CNPD destaca que, por traduzirem restrições a direitos, liberdades e garantias, máxime dos direitos fundamentais ao respeito pela vida privada e familiar e à proteção de dados pessoais, em violação grosseira do princípio da proporcionalidade, se afiguram ser inconstitucionais as seguintes normas da Proposta de Lei: os incisos *ii.* e *iii.* da alínea *d)* do artigo 3.º; o n.º 2 do artigo 10.º, o artigo 11.º, o artigo 17.º e o artigo 18.º.

162. Finalmente, a CNPD toma a liberdade de assinalar que, na sua perspetiva, o impacto que a presente Proposta de Lei tem nos direitos fundamentais dos cidadãos e as deficiências estruturais que esta apresenta na pretensa regulação de tratamentos de dados pessoais altamente restritivos de direitos, liberdades e garantias reclamam um debate profundo e alargado das diferentes disposições legais.

Aprovado na reunião de 4 de novembro de 2021

Filipa Calvão (Presidente)