
Projeto de Lei n.º 531/XVII/1ª - Primeira alteração à Lei n.º 95/2021, de 29 de dezembro (Regula a utilização e o acesso pelas forças e serviços de segurança e pela Autoridade Nacional de Emergência e Proteção Civil a sistemas de videovigilância para captação, gravação e tratamento de imagem e som), em matéria de prevenção da prática de atos terroristas

Proc. 2026/GAVPM/2203

04/05/2026

PARECER

1. Objeto

Pela Direção de Apoio Parlamentar da Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias da Assembleia da República foi remetido ao Conselho Superior da Magistratura o Projeto de Lei *supra* identificado, que visa alterar a Lei n.º 95/2021, de 29 de dezembro (Regula a utilização e o acesso pelas forças e serviços de segurança e pela Autoridade Nacional de Emergência e Proteção Civil a sistemas de videovigilância para captação, gravação e tratamento de imagem e som), em matéria de prevenção da prática de atos terroristas.



2. Análise formal

2.1. Analisada a exposição de motivos do projeto de lei em referência, para explicitação dos fundamentos que estiveram na génese da alteração proposta, ali refere-se que:

«Em 6 de setembro de 2021, o XXII Governo constitucional apresentou à Assembleia da República a Proposta de Lei n.º 111/XIV-2.^a, cujo objeto foi a regulação da utilização e o acesso, pelas forças e serviços de segurança e pela Autoridade Nacional de Emergência e Proteção Civil, a sistemas de videovigilância para captação, gravação e tratamento de imagem e som.

Esta iniciativa deu origem à Lei n.º 95/2021, de 29 de dezembro, a nova lei da videovigilância, que – tal como consta do título da mesma – revogou a Lei n.º 1/2005, de 10 de janeiro, em razão dos mais de 15 anos de vigência desta, da sua alteração por vários diplomas legais e, ainda, por se mostrar necessário adequar a lei da videovigilância aos avanços tecnológicos e às alterações das características técnicas dos novos sistemas disponíveis no mercado e, bem assim, à evolução do regime jurídico da proteção dos dados pessoais em consequência da entrada em vigor do Regulamento Geral de Proteção de Dados (RGPD), aprovado pelo Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, e das leis n.ºs 58 e 59/2019, de 8 de agosto.

A Lei n.º 95/2021 difere da Proposta de Lei n.º 111/XIV num aspeto que se reveste de importância capital em matéria de prevenção do terrorismo: enquanto nesta se previa a possibilidade de tratamento de dados biométricos, para efeitos de prevenção de atos terroristas, a Lei n.º 95/2021 permite o tratamento de dados através de um sistema de gestão analítica dos dados captados, inclusivamente para prevenção de atos terroristas, mas proíbe terminantemente a captação e tratamento de dados biométricos.

É um facto que Portugal tem estado imune a atentados terroristas como os que flagelaram outros Estados europeus, pelo que o grau de ameaça terrorista tem tido um nível que se manteve no moderado (grau 4) até 2023, aquando do ataque do Hamas a Israel, ocasião em que passou a significativo (grau 3) no qual se mantém até agora¹.

Efetivamente, alguns sinais de aumento do nível de ameaça terrorista mereceram atenção por parte da Europol, que advertiu para um risco mais elevado de situações de

¹https://cnnportugal.iol.pt/terrorismo-portugal/terrorismo/grau-de-ameaca-terrorista-para-portugal_mantem-se-em-grau-3-mas-esta-em-permanente-reavaliacao-devido-ao-conflito-no-medio-oriente/20260304/69a89b07d34edcee7c617dc1



terrorismo na União Europeia devido à escalada do conflito no Médio Oriente², que coloca todo o território da UE num nível elevado de ameaça terrorista e de extremismo violento.

A Estratégia Nacional de Combate ao Terrorismo (ENCT) foi aprovada pela Resolução do Conselho de Ministros n.º 40/2023, de 3 de maio, e está organizada em torno de quatro eixos estratégicos (prevenção, proteção, perseguição e resposta). No que respeita ao eixo prevenção, é dito que este eixo «visa antecipar e detetar potenciais ameaças terroristas, conhecendo e identificando as causas e tendências que determinam o surgimento de processos de radicalização, adesão e recrutamento, de modo a prevenir atos que configurem infrações terroristas.», e que se desenvolve através de um conjunto de linhas de ação, entre as quais se contam «vi) Intensificar a cooperação, no plano operacional, entre todas as entidades competentes;» e «vii) Promover a cooperação internacional, a colaboração e o desenvolvimento de uma ação externa comum, através da partilha de informações relacionadas com a atividade terrorista a nível global.».

O Chega considera estas linhas de ação dificilmente realizáveis sem recurso à captação e tratamento de dados biométricos, estranhando-se a falta de alusão a esta realidade quando se sabe que o Governo que aprovou esta ENCT foi praticamente o mesmo que apresentou a Proposta de Lei n.º 111/XIV. Aliás, sem recurso aos dados biométricos e à inteligência artificial, a ENCT dificilmente poderá ser aplicada.

A eficácia da videovigilância na prevenção do terrorismo ficou plenamente demonstrada nos atentados de Londres, em 2005: foi o sistema de CCTV londrino que permitiu identificar quais tinham sido os terroristas da primeira vaga de atentados, bem como proceder à detenção dos que se preparavam para levar a cabo uma segunda vaga de atentados na cidade. Também nos atentados em Paris e Saint-Denis, em 16 de novembro 2015, e em Bruxelas, em 2016, a videovigilância foi determinante para a captura dos terroristas, e levou as autoridades francesas a reforçar o seu dispositivo de videovigilância em todo o seu território. Idêntica atitude tomaram as autoridades alemãs, após os atentados num mercado de Natal, na Cidade Ocidental de Berlim, em dezembro de 2017.

A videovigilância tem uma importância determinante na prevenção de atos terroristas, constituindo uma importante arma no arsenal do combate ao terrorismo.

²<https://sicnoticias.pt/mundo/2026-03-06-europol-alerta-para-maior-risco-de-terrorismo-na-uedevido-ao-conflito-no-medio-orient-5464414d>



É fundamental, para tanto, que seja apetrechada com os recursos que lhe permitam desenvolver todas as suas potencialidades, para que Portugal não continue a ser o elo mais fraco do Espaço Schengen, no que concerne a meios de prevenção do terrorismo».

2.2. Com tal enquadramento motivador, o Grupo Parlamentar do CHEGA apresentou à Assembleia da República o seguinte Projeto de Lei:

Artigo 1.º

Objeto

A presente lei procede à primeira alteração à Lei n.º 95/2021, de 29 de dezembro, permitindo a captação e tratamento de dados biométricos para o efeito de prevenção de atos terroristas.

Artigo 2.º

Aditamento à Lei n.º 91/2025³, de 29 de dezembro

O artigo 16.º da Lei n.º 95/2021, de 29 de dezembro, passa a ter a seguinte redação:

“Artigo 16.º

[...]

1 – [...]

2 – Para efeitos do disposto na alínea e) do n.º 1 do artigo 3.º, é permitida a captação e tratamento de dados biométricos.”

Artigo 3.º

Entrada em Vigor

A presente lei entra em vigor no dia seguinte ao da sua publicação.

Analisando.

³ É evidente o lapso no Projeto de Lei na identificação do diploma em causa, pois trata-se da Lei n.º 95/2021, de 29.12.



A iniciativa legislativa é composta por 3 artigos, em que o primeiro define o objeto da proposta legislativa; o segundo determina a alteração ao artigo 16.º da Lei n.º 95/2021, de 29 de dezembro e o terceiro define o momento em que a alteração preconizada deve entrar em vigor.

3. Apreciação

Nos termos do artigo 149.º, n.º 1, alínea i), do Estatuto dos Magistrados Judiciais (aprovado pela Lei n.º 21/85, de 30 de julho, com as alterações introduzidas pela Lei n.º 67/2019, de 27 de agosto) compete ao Conselho Superior da Magistratura emitir parecer sobre diplomas legais relativos à organização judiciária e à matéria estatutária e, em geral, sobre matérias relativas à administração da justiça.

Em sentido idêntico dispõe o artigo 155.º, alínea b), da Lei da Organização do Sistema Judiciário (aprovada pela Lei n.º 62/2013, de 26 de agosto, com as alterações introduzidas pela Lei n.º 40-A/2016, de 22 de dezembro)

No estrito cumprimento das mencionadas normas legais, o Conselho Superior da Magistratura, enquanto órgão de gestão e disciplina da magistratura judicial, e atento o princípio constitucional da separação de poderes, tem vindo a abster-se de tomar posição sobre questões que se prendam com opções de cariz eminentemente político ou que extravasam as atribuições do poder judicial e incumbem exclusivamente ao poder legislativo.

3.1 Assente o âmbito de análise técnica do parecer que nos cumpre emitir, importa começar por sublinhar que se trata de uma alteração que reflete uma opção política, sem reflexo direto na organização judiciária, na matéria estatutária ou na administração da justiça globalmente considerada.

Todavia, apesar de estamos perante uma alteração “simples” (na medida em que envolve “apenas” um número de um artigo), esta tem um potencial de grande impacto.

Com efeito, tratando-se de matéria conexa com os Direitos, Liberdades e Garantias (artigos 17.º e ss. da Constituição da República Portuguesa), com reflexos diretos sobre segmentos do ordenamento jurídico, nomeadamente o relacionado com o acesso pelas forças e serviços de segurança e pela Autoridade Nacional de Emergência e Proteção Civil a sistemas de videovigilância para captação, gravação e tratamento de imagem e som,



entendemos que se impõe alertar o legislador, pois se suscitam relevantes questões jurídicas, constitucionais e de proteção de dados.

3.2 A atual redação do artigo 16.º da Lei n.º 95/2021, de 29 de dezembro, é a seguinte:

Artigo 16.º

Recolha e tratamento de dados

1 - Para os fins previstos do artigo 3.º, o tratamento dos dados pode ter subjacente um sistema de gestão analítica dos dados captados, por aplicação de critérios técnicos, de acordo com os fins a que os sistemas se destinam.

2 - Para efeitos do disposto no número anterior, não é permitida a captação e tratamento de dados biométricos.

Com o Projeto de Lei, a redação deste preceito passará a ser a seguinte (alteração a **negrito**):

Artigo 16.º

Recolha e tratamento de dados

1 - Para os fins previstos do artigo 3.º, o tratamento dos dados pode ter subjacente um sistema de gestão analítica dos dados captados, por aplicação de critérios técnicos, de acordo com os fins a que os sistemas se destinam.

2 - **Para efeitos do disposto na alínea e) do n.º 1 do artigo 3.º, é permitida a captação e tratamento de dados biométricos.**

Importa lembrar que, nos termos do artigo 2.º, n.º 2 desta Lei n.º 95/2021, de 29.12, deve entender-se por «captação e tratamento de dados biométricos» o previsto no artigo 3.º da Lei n.º 59/2019, de 08 de agosto (que aprovou as regras relativas ao tratamento de dados pessoais para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais, transpondo a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016), no sentido de que:

- «Tratamento» consiste numa operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não



automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, por difusão ou por qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição;

- «Dados biométricos» são dados pessoais resultantes de um tratamento técnico específico, relativos às características físicas, fisiológicas ou comportamentais de uma pessoa singular, que permitam ou confirmem a sua identificação única, tais como imagens faciais ou dados dactiloscópicos.

Note-se ainda que a alínea e), do n.º 1, do artigo 3.º deste diploma (não sujeita a qualquer alteração), dispõe que:

«1- Os sistemas de videovigilância apenas podem ser usados para a prossecução dos fins previstos na Lei de Segurança Interna, aprovada pela Lei n.º 53/2008, de 29 de agosto, e em concreto para: (...) e Prevenção de atos terroristas; (...)».

3.3 Em síntese, o Projeto de Lei n.º 531/XVII/1.^a, apresentado pelo Grupo Parlamentar do CHEGA, propõe uma primeira alteração à Lei n.º 95/2021, de 29.12, para permitir a captação e tratamento de dados biométricos no contexto da prevenção de atos terroristas.

Esta Lei n.º 95/2021, de 29.12, regula a utilização e o acesso, pelas forças e serviços de segurança e pela Autoridade Nacional de Emergência e Proteção Civil (ANEPC), a sistemas de videovigilância para captação, gravação e tratamento de imagem e som, tendo revogado a antiga Lei n.º 1/2005, de 10.01, reforçado os princípios da proporcionalidade, necessidade e adequação nesta matéria e proibido expressamente a captação e tratamento de dados biométricos, em linha com o Regulamento Geral de Proteção de Dados (RGPD) e com a Lei n.º 59/2019, de 08.08, que regula o tratamento de dados pessoais para fins de prevenção e repressão criminal.

Nos termos do artigo 3.º da Lei n.º 95/2021, a videovigilância pode ser usada, entre outros fins, para prevenção de atos terroristas, mas sem recurso a dados biométricos - apenas através de sistemas analíticos de imagem (ex.: deteção de comportamentos, padrões de movimento, etc...).



Atenta a Exposição de Motivos e o teor da alteração, o Projeto de Lei visa autorizar a recolha e análise biométrica (por exemplo, reconhecimento facial ou de marcha) para fins de «prevenção de atos terroristas».

A definição de terrorismo no ordenamento jurídico português encontra-se essencialmente na Lei n.º 52/2003, de 22 de agosto (Lei de Combate ao Terrorismo), atualizada mais recentemente pela Lei n.º 2/2023, de 16 de janeiro, que transpôs a Diretiva (UE) 2017/541, sendo complementada por disposições no Código de Processo Penal e em legislação especial de combate à criminalidade organizada e de organização da investigação criminal.

Sucedendo que, se a intenção é excecionar a recolha e uso daqueles dados para efeitos de prevenção do terrorismo, seria aconselhável que a alteração legislativa fosse particularmente clara e rigorosa nesse sentido, mantendo ou ressaltando a proibição da captação e tratamento de dados biométricos para os demais fins previstos no artigo 3.º do mesmo diploma.

Com efeito, ao suprimir a anterior redação (que para todos os efeitos -incluindo prevenção do terrorismo- não permitia a captação e tratamento de dados biométricos) e apenas aludir à permissão de captação e tratamento de tais dados para efeitos do disposto na alínea e) do n.º 1 do artigo 3.º, fica em aberto qual o restante âmbito da captação e tratamento de dados biométricos.

Apesar de uma interpretação sistémica e integrada deste diploma com a Lei n.º 59/2019, de 08.08 e o Regulamento (UE) n.º 679/2016, de 27 de abril (RGPD) permitir concluir que a recolha e tratamento de tais dados, fora da permissão ora introduzida, não será permitida, a alteração legislativa introduziria, desnecessariamente, uma perturbação na coerência e consistência deste quadro jurídico.

Dito de outro modo, se a intenção (como parece decorrer da Exposição de Motivos) é criar uma exceção à proibição “geral”, então ter-se-ia de manter a proibição de cariz genérico que consta da atual redação do n.º 2 do artigo 16.º (acrescentando apenas a exceção).

Neste sentido, e indo de encontro às razões elencadas para a alteração sugerida, seria mais claro e rigoroso manter a proibição que consta do atual n.º 2 do artigo 16.º, aduzindo a exceção da possibilidade de captação e tratamento de dados biométricos para efeitos do disposto na alínea e) do n.º 1 do artigo 3.º.



3.4 Sucede que, mesmo admitindo que se trata “apenas” de uma exceção, tal alteração legislativa não se mostra inócua, suscitando reflexões que não se mostram vertidas na Exposição de Motivos ou esclarecidas no exato teor da iniciativa legislativa.

Desde logo, porque a um reforço da vigilância pública (desde logo a autorização de sistemas com reconhecimento facial poderia ampliar substancialmente o alcance da videovigilância em Portugal) está associado um risco acrescido para alguns direitos fundamentais (decorrentes da invasão potencial da privacidade e possibilidade de erro, discriminação e abuso tecnológico).

Pode mesmo sustentar-se estar aqui o embrião de uma mudança estrutural de paradigma, alterando-se o atual modelo restritivo para um modelo permissivo quanto à biometria no espaço público.

É que esta singela alteração ao n.º 2 do artigo 16.º, da Lei n.º 95/2021, de 29 de dezembro, passa a permitir expressamente a captação e tratamento de dados biométricos sem definir limites concretos (*maxime* operacionais ou de delimitação espacial/temporal); tipificar situações específicas; definir critérios de proporcionalidade concretos; exigir explicitamente autorização judicial ou estabelecer salvaguardas adicionais.

Estando em “confronto”, por um lado, o direito à imagem, à voz e à vida privada, enquanto concretizações do direito à reserva da intimidade da vida privada, com consagração no artigo 26.º, n.º 1, da Constituição da República Portuguesa (CRP) e, por outro lado, o direito à segurança, com assento constitucional no artigo 27.º, impunha-se assegurar o justo equilíbrio na sua concordância, como estipula o n.º 2 do artigo 18.º da CRP.

Como se pode ler no emblemático acórdão do Supremo Tribunal de Justiça de 28.09.2011 (Proc. n.º 22/09.6YGLSB.S2, *in* www.dgsi.pt):

«IV- A segurança é um elemento essencial da vida dos cidadãos, consubstanciando-se num direito à existência de um clima de paz e confiança mútua, que lhes permite o livre exercício dos seus direitos individuais, sociais e políticos.

V- O direito à segurança não sendo um direito absoluto é, todavia, um direito constitucional que, qualitativamente, se situa num nível equiparável a outros direitos fundamentais que, pelo simples facto de o serem, não deixam de estar sujeitos a uma ponderação de valores. O Direito à segurança é uma garantia de outros direitos fundamentais e, simultaneamente, um direito inscrito no património de cada cidadão.



VI- Um dos pilares fundamentais do Estado de Direito é a relação equilibrada construída entre segurança e democracia ou entre segurança e direitos fundamentais. O Tribunal Europeu dos Direitos do Homem tentou, em diversas decisões, responder a esta questão fundamental, reconhecendo que, numa sociedade democrática, os interesses da segurança nacional prevalecem sobre os interesses individuais, mas tornando, também, claro os limites que não podem ser ultrapassados em nome da segurança, nomeadamente em termos de inserção naquelas bases de dados. Assim, o poder de vigiar em segredo os cidadãos só pode ser tolerado na medida estritamente necessária à salvaguarda das instituições democráticas. É o grau mínimo de protecção requerido pela prevalência do direito numa sociedade democrática

VIII- A videovigilância surge, simultaneamente, como uma imposição das exigências de segurança, uma forma do desenvolvimento das tecnologias de segurança e também uma consequência de novas formas de abordagem do fenómeno da criminalidade. A sua utilização no domínio da segurança é muitas vezes o ponto de encontro ou o resultado da aplicação de estratégias que visam o controle do espaço em que o cidadão se realiza e, nomeadamente, o espaço urbano e a sua gestão».

Tendo em conta estes breves considerandos e a especialíssima natureza dos dados biométricos (que, além da *supra* citada definição legal para onde este diploma expressamente remete, são também, à luz do artigo 4.º, n.º 14 do RGPD, dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos), importa lembrar que o artigo 6.º da Lei n.º 59/2019, de 08.08, proíbe o seu tratamento, salvo em casos de absoluta necessidade e mediante salvaguardas adicionais definidas por lei, nomeadamente apenas se for autorizado por lei; se destinar a proteger os interesses vitais do titular dos dados ou de outra pessoa singular; ou estiver relacionado com dados manifestamente tornados públicos pelo titular dos dados.

Lembramos que em 28.09.2023, a Comissão Nacional de Protecção de Dados (CNPD) já tinha advertido, em parecer sobre uma alteração autónoma da mesma lei⁴, que a introdução de novas finalidades de vigilância sem estudo de impacto ou base legal clara era contrária aos princípios da proporcionalidade e minimização de dados, sendo estes argumentos reforçados no caso dos dados biométricos, pois representam o tipo mais intrusivo de informação pessoal.

⁴ file:///Users/marcosfilipegoncalves/Downloads/Parecer_2023_86.PDF



Sendo igualmente claro que o Projeto de Lei terá também de se compatibilizar com o artigo 35.º da CRP (além do sobredito artigo 26.º), não se pondo em causa a intenção da iniciativa legislativa e a necessidade de assegurar medidas atuais e eficazes na luta contra o terrorismo, entendemos que qualquer Projeto de Lei que restrinja/comprima esses direitos deveria refletir uma concreta base de necessidade e proporcionalidade claramente comprovada; delimitar finalidades, prazos e órgãos responsáveis, além de assegurar a sua sujeição a controlo jurisdicional e administrativo.

De igual forma, para garantir a sua conformidade à Lei Fundamental e ao Direito da União, deveria ponderar-se para este uso excepcional de dados biométricos a proibição expressa de qualquer vigilância massiva (proibição de *scanning* indiscriminado de multidões); a existência de garantias reforçadas de dados (*vg.* limitação de conservação, auditoria, proibição de *profiling* sensível) e a previsão de uma avaliação de impacto obrigatória (reforçando a *accountability*).

Sem disposições detalhadas sobre tais garantias, a autorização genérica da recolha de dados biométricos⁵ (ainda que excepcional), além de potencialmente desconforme face ao Direito Europeu (como vimos quanto ao RGPD e analisaremos de seguida relativamente ao RIA - AI Act), poderá levantar questões de inconstitucionalidade, relacionadas, além do mais, com os princípios da determinação legal e da reserva de lei restritiva de direitos fundamentais.

Assim, por forma a ganhar consistência e antecipar discussões quanto à sua conformidade constitucional e com o Direito Europeu, seria aconselhável que o diploma refletisse a necessária ponderação destes considerandos e os tente acautelar.

3.5 Lembramos também que qualquer sistema de videovigilância terá de ser previamente autorizado e acompanhado pela Comissão Nacional de Proteção de Dados (artigo 5.º, n.º 3 da Lei 95/2021, de 29.12), sendo expectável que a CNPD solicite, além do mais, uma avaliação de impacto específica para dados biométricos e limites estritos de funcionamento e armazenamento.

⁵ As exceções previstas em outros ordenamentos jurídicos europeus são densamente regulamentadas e com controlo externo obrigatório.



Neste sentido, a exceção que se pretende introduzir deveria igualmente ser acompanhada de disposições sobre tais procedimentos, a fim de evitar que a aplicação prática da nova lei seja juridicamente bloqueada a jusante.

3.6 Acresce que esta iniciativa igualmente aconselha cautelas de compatibilidade com o Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho de 13 de junho de 2024 (RIA - AI Act) que cria regras harmonizadas em matéria de inteligência artificial e que altera os Regulamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e as Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regulamento da Inteligência Artificial)⁶.

Entre o mais, o AI Act proíbe ou restringe fortemente o uso de sistemas de Inteligência Artificial (IA) de identificação biométrica remota em tempo real em espaços públicos, podendo apenas ser autorizado em casos muito específicos, como: prevenção ou resposta a ameaças terroristas concretas; busca de vítimas de crimes graves e perseguição de suspeitos de crimes graves, mediante autorização judicial prévia ou controlo jurisdicional posterior.

As aplicações de IA de “alto risco”, incluindo videovigilância com reconhecimento facial, exigem avaliação de conformidade, registo europeu, documentação técnica e supervisão rigorosa pelas autoridades competentes (em Portugal, a Comissão Nacional de Proteção de Dados).

É importante lembrar que a recolha de dados biométricos (como reconhecimento facial) só será admissível em contextos de prevenção ou investigação de terrorismo; com autorização judicial prévia; sob fiscalização da CNPD e da Inspeção-Geral da Administração Interna (IGAI) e para finalidades estritamente delimitadas (em respeito pelos princípios da necessidade, proporcionalidade e minimização dos dados).

Acresce que a conformidade prática com tal regulamento por parte do Estado Português dependerá de estar assegurada a supervisão efetiva pela CNPD e IGAI sobre o uso dos sistemas; a garantia de que não há armazenamento massivo ou tratamento preditivo

⁶ Visa assegurar que a IA utilizada no espaço europeu seja segura, transparente, ética e respeitadora dos direitos fundamentais, e, ao mesmo tempo, promover a inovação e reforçar a competitividade da Europa no domínio da IA. O regulamento adota uma abordagem proporcional, baseada no nível de risco que diferentes aplicações de IA podem representar para os direitos dos cidadãos ou para a sociedade.



de dados sensíveis fora dos casos autorizados; da transparência e auditoria sobre os algoritmos usados, tal como exigido pelo AI Act para sistemas de alto risco.

Seria, pois, avisado, que uma iniciativa legislativa como a presente, que redundaria numa autorização genérica para captação e tratamento de dados biométricos, acautele os sobreditos aspetos (o que implica uma intervenção mais global e detalhada, inclusive em diplomas conexos).

Aliás, em termos comparados, julgamos que o problema não será a existência de uma exceção para recolha e uso de biometria, mas a de uma permissão nesse sentido sem densidade normativa equivalente à dos outros países da União (onde o legislador nacional poderá encontrar inspiração).

3.7 Por último, existe um lapso na epígrafe do artigo 2.º ao aludir à Lei n.º “91/2025”, quando é evidente que se pretende referir a Lei n.º 95/2021, de 29 de dezembro.

4. Conclusão

O presente Projeto de Lei está de acordo com as motivações que o determinaram, consubstanciando uma opção de política legislativa, todavia, parece-nos aconselhável a sua reformulação, com a ponderação das observações acima assinaladas, para garantir a sua compatibilidade com o quadro normativo nacional e europeu (*maxime* em matéria de proteção de dados e direitos fundamentais).

Sublinhamos que apesar da sua dimensão singela, a alteração legislativa visada tem potencial para romper o equilíbrio estabelecido pelo legislador em 2021, e embora a adoção de um modelo mais securitário seja uma legítima opção política, deve ser acompanhada do devido enquadramento, por forma a não criar uma entropia no ordenamento jurídico.

Entendemos que só configurando a utilização de biometria como um instrumento excepcional, controlado e juridicamente densificado estará assegurada a sua validade constitucional e europeia.



**Marcos Filipe
Nunes Pires
Gonçalves**
Adjunto/a

