REVISTA DO CEJUR/TJSC: PRESTAÇÃO JURISDICIONAL
JOURNAL OF ADMINISTRATIVE JUSTICE SYSTEM
E-ISSN: 2319-0884
OPEN ACCESS
PODER JUDICIÁRIO de Santa Catarina

DA VIGILÂNCIA BIOMÉTRICA NO ORDENAMENTO DA UNIÃO EUROPEIA

(para fins de segurança em espaços acessíveis ao público) – Uma perspetiva portuguesa especialmente destinada ao Brasil[1]

Manuel David Masseno[2]

RESUMO

Objetivo: Analisar os regimes jurídicos aplicáveis à vigilância biométrica dos espaços acessíveis ao público para fins de segurança pública e de justiça criminal na União Europeia, atendendo também aos processos legislativos em andamento, desde Portugal, mas com uma abertura ao diálogo com o Brasil.

Metodologia: Foi seguindo fundamentalmente o método jurídico-dogmático, embora com aberturas aos métodos hermenêutico, comparativo e aos resultados do método sociojurídico.

Resultados: O artigo avalia os riscos para os Direitos Fundamentais resultantes da utilização da biometria e do inerente tratamento automatizado de dados para a identificação dos cidadãos nos espaços públicos à luz da regulação atual sobre Proteção de Dados e da futura IA - Inteligência Artificial na União Europeia, tendo também em consideração as situações regulatórias em Portugal e no Brasil.

Contribuições: O estudo mostrou como as escolhas legislativas em matéria de tecnologias, especialmente no respeitante à IA, podem constranger as Liberdades Cívicas e promover o controle pelos Poderes Públicos para além dos limites do Estado de Direito.

Palavras-Chave: Proteção de Dados. Segurança Pública. União Europeia. Vigilância Biométrica.

ARTIGO CONVIDADO
Aceito em: 17 de julho. 2023
DOI: https://doi.org/10.37497/revistacejur.v11i00.402

[1] Este texto correspondente à intervenção na 6ª Sessão do Ciclo de Webinars "Smart Cities and Law, E-Governance and Rights", a qual teve por objeto "Cidades Inteligentes, Património Cultural e Turismo Sustentável", no Painel "Direito(s), Cidades e Turismo Inteligente", realizado na Escola de Direito da Universidade do Minho, em Braga, no dia 17 de março de 2023, no âmbito do Projeto (Horizonte Europa) "Smart Cities and Law, E.Governance and Rights: Contributing to the definition and implementation of a Global Strategy for Smart Cities", coordenado pela Prof.ª Isabel Celeste Fonseca, estando a versão original em publicação pela Universidade do Minho. Esta intervenção seguiu de perto, especificando, a "Conferencia Inaugural" proferida na "III Jornada sobre el marco jurídico de la Ciencia de Datos: perspectivas de la inteligencia artificial", organizada pela *Universitat Politècnica de Valencia* no dia17 de novembro de 2022. Entretanto e antecipando a publicação das respetivas *Actas*, o texto foi publicado Manuel David MASSENO (2022 [b]). Como, por razões de equilíbrio, as referências feitas à Doutrina portuguesa foram então limitadas, neste terei apenas em consideração a Doutrina nacional, desde que publicada em Acesso Aberto. Esta versão, pensada como uma proposta de diálogo com os Colegas brasileiros, contem anotações adicionais relativas às correspondentes Fontes legislativas e Doutrina, para tal tendo contado com o especial apoio dos Professores Melina Ferracini de Moraes, Aline Macohin, Cleórbete Santos e Dierle Nunes, as quais muito agradeço.

[2] Professor Adjunto do IPBeja - Instituto Politécnico de Beja (Portugal), onde também integra as Coordenações do Laboratório UbiNET – Segurança Informática e Cibercrime e do MESI – Mestrado em Engenharia de Segurança Informática, sendo ainda o seu Encarregado da Proteção de Dados. Além de ser Membro convidado do PDPC – Centro de estudos e análise da privacidade e proteção de dados da Universidade Europeia, de Lisboa, pertence à EDEN – Rede de Especialistas em Proteção de Dados da Europol – Agência Europeia de Cooperação Policial e integra a Comissão permanente de Direito Digital da Seção de Santa Catarina da Ordem dos Advogados do Brasil. **Email:** mdmasseno@gmail.com **Orcid:** https://orcid.org/0000-0001-8861-0337

ON BIOMETRIC SURVEILLANCE IN EUROPEAN UNION LAW

(for the Security in Publicly Accessible Spaces) – A Portuguese Perspective Especially towards Brazil

ABSTRACT

Objective: To analyse the legal frameworks of biometric surveillance of publicly accessible spaces for public security and criminal justice purposes in the EU - European Union, also taking into consideration the current legislative procedures, from Portugal, also in order to open a dialog with Brazil.

Methodology: The doctrinal legal research method was the mostly followed, but the hermeneutic and the comparative methods also had a role, the same for the outcomes of sociolegal method.

Results: This paper evaluates the risks for Fundamental Rights coming from the use of biometrics and the inherent automatised processing of data for the identification of citizens in publicly accessible spaces in light of the EU current legislation on Personal Data and the future AI - Artificial Intelligence Act, having in mind the regulatory situations in Portugal and Brazil.

Contributions: The research showed how the legislative choices related to technologies, specially involving AI, may constrain Civil Liberties and promote the control by Public Authorities beyond the boundaries of the Rule of Law.

Keywords: Biometric Surveillance. Data Protection. European Union. Public Security.

1 – Para um enquadramento das questões

Antes de mais e como tem evidenciado o CEPD – Comité Europeu para a Proteção de Dados, é fundamental destrinçar dentro dos sistemas de videomonitoramento os que procedem ao tratamento de "dados biométricos"[3].

Com efeito, destes emergem riscos acrescidos para os direitos e liberdades dos titulares dos dados, ao serem procedimentos automatizados, quase sempre com recurso bases de dados geridas por sistemas de IA – Inteligência Artificial.

Daí resultando um ponto de fricção, inclusive fraturante, nas Sociedades Democráticas, entre a garantia das Liberdades, incluindo a inerente ao anonimato no espaço público, e a Segurança, indispensável à efetividade daquelas. Por outras palavras, está presente a ameaça de passarmos a ter de viver numa Sociedade de Vigilância, sob o controle permanente de Poderes, tanto públicos quanto privados, inclusive articulados

[3] A identificação específica dos riscos inerentes a esta diferença qualitativa remonta ao *Parecer 3/2012 sobre a evolução das tecnologias biométricas*, adotado em 27 de abril pelo Grupo de Trabalho do Artigo 29.º, predecessor do CEPD, ao se seguiram, desde uma perspetiva simétrica, as *Diretrizes n.º 3/2019 relativas ao tratamento de dados pessoais através de sistemas de videovigilância* [videomonitoramento] (Versão 2.1), de 26 de fevereiro de 2020, já do CEPD.

entre si de modos muitas vezes destituídos de qualquer transparência e sem terem os cidadãos a possibilidade de os escrutinarem[4].

Enquanto, de acordo com o *RGPD – Regulamento Geral sobre a Proteção de Dados* da União Europeia[5] (Art.º 3.º 14) e com a *Diretiva LE* – Diretiva sobre a Proteção de Dados na Segurança Pública e na Justiça Criminal[6] (Art.º 3.º 13), por "«Dados biométricos» [têm-se: os]

> dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular [natural] que permitam ou confirmem a identificação única dessa pessoa singular [natural], nomeadamente imagens faciais ou dados dactiloscópicos" [enquanto a Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (*LGPD*), qualifica o "dado […] biométrico" enquanto "dado pessoal sensível", Art. 5º II, mas não o define]

O que implica identificar tais dados com os constantes duma base, através de processamentos automatizados. Um procedimento que diverge, até em termos radicais, do videomonitoramento "simples", assente na observação humana, ao facilitar a «definição de perfis» dos titulares, por tal se entendendo:

> "[…] qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos

[4] Sobre estas questões, desde perspetivas disciplinares diferentes e com uma ênfase crescente na vigilância biométrica, têm muito interesse os estudos de Ana VAZ (2007), de Catarina FRÓIS (2014) e (2011), de Laura NEIVA (2020), de José FONTES (2022) e de Manuel Poêjo TORRES & Afonso de Freitas DANTAS (2020), além das inquietações conclusivas de Lurdes DIAS ALVES (2019) e das avaliações críticas de Vera Lúcia RAPOSO (2021) e de Rui Soares PEREIRA (2022), este em termos panorâmicos; bem como a minha análise, Manuel David MASSENO (2022 [b]) e, sobretudo, as reflexões de âmbito mais geral e de Teresa Coelho MOREIRA & Francisco C. Pacheco de ANDRADE (2016). [No que se refere ao Brasil, têm um especial interesse para estas questão os recentes estudos interdisciplinares de Camila Berlim SCHNEIDER & Pedro Fauth Manhães MIRANDA (2019), de Ramon Silva COSTA & Bianca KREMER (2022), de Paulo Victor MELO & Paulo SERRA (2022) e de Fernanda Miler Lima PINTO (2023); assim como as reflexões com um maior grau de abstração de Rosane Leal da SILVA & Fernanda dos Santos Rodrigues da SILVA (2019), de Ana Julia Pozzi ARRUDA, Ana Paula Bougleux Andrade RESENDE & Fernando Andrade FERNANDES (2021), assim como as de Vinícius de Almada MOZETIC & Diego Roberto BARBIERO (2022) e de Érica Nascimento Pinheiro VARGAS & Mônica Matos RIBEIRO (2023) e, ainda, as análise sobretudo técnico-jurídicas de Pedro Augusto FRANCISCO, Louise Marie HUREL & Mariana Marques RIELLI (2020) de Eduarda Costa ALMEIDA (2023) e de Fernando Andrade FERNANDES & Ana Paula Bougleux Andrade RESENDE (2023)]

[5] Por extenso, Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares [naturais] no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (*Regulamento Geral sobre a Proteção de Dados*).

[6] A Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativa à proteção das pessoas singulares [naturais] no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho.

> pessoais de uma pessoa singular [natural], nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações" (Art.º 4.º 4) do *RGPD* e Art.º 3.º 4) da *Diretiva LE*) [A LGPD refere o "perfil" no Art. 12 § 2º e no *caput* do Art. 20, igualmente sem o definir].

Daí resultando riscos acrescidos para os Direitos e as Liberdades e até um alarme social maior que os associados à conservação e acesso ao metadados resultantes das comunicações eletrónicas[7]. Sobretudo se uma tal vigilância ocorrer indiscriminadamente e em espaços acessíveis ao público, mais ainda se em territórios ou cidades inteligentes, com múltiplos sensores interconectados[8]. O que ainda poderá ser mais gravoso se estiver efetivamente articulado com a referida "definição de perfis" ou a sistemas de "classificação social", sobretudo se generalizados e com aptidões preditivas[9].

Efetivamente, para além do "respeito pela vida privada e familiar" e da "proteção de dados", com a utilização de tais sistemas ficam em causa restrições a outras liberdades, como a "de pensamento, de consciência e de religião", a "de reunião e de associação", a "de circulação e de permanência" e até a "presunção de inocência e direitos de defesa", sempre sujeitas ao "princípio da proporcionalidade" (Art.ºs 7.º, 8.º, 10.º, 12.º, 45.º, 48.º e 52.º n.º 1 da *CDFUE – Carta dos Direitos Fundamentais da União Europeia*).

2 – Algumas considerações sobre o regime vigente

Como verificámos, o RGPD disciplina a o tratamento de "dados biométricos" em geral, incluindo vigilância biométrica, enquanto tratamento duma "categoria especial de dados"[10].

[7] Como os identificados pelo TFUE – Tribunal de Justiça da União a partir dos Acórdãos *Digital Rights Ireland* (Processos apensos C-293/12 e C-594/12, de 8 de abril de 2014) e *Tele2 Sverige* (Processo C-203/15, de 21 de dezembro de 2016), enquanto *leading cases*, cujo sentido e implicações, inclusive para os Ordenamentos nacionais, designadamente para o português, foram estudados de imediato por David Silva RAMALHO & José Duarte COIMBRA (2015) e por Alessandra SILVEIRA & Pedro Miguel FREITAS (2017), sendo também de referir a análise prospetiva, também a este respeito, resultante do conhecimento direto das dinâmicas do Tribunal do Luxemburgo, de José L. da Cruz Vilaça (2019).

[8] Como explicitámos a propósito do expoente maior de tais territórios, os "Destinos Turísticos Inteligentes", inclusive no que se refere ao Património Natural, em Manuel David MASSENO & Cristiana Teixeira SANTOS (2018 [a]) e em (2018 [b]), com o segundo estudo a ser apresentado como "a referência jurídica" na União Europeia https://smarttourismdestinations.eu/digital-library/.

[9] Como sublinham, colocando a China como parâmetro distópico, Vera Lúcia RAPOSO (2022) e, mais ainda, Maria Raquel GUIMARÃES (2022).

[10] Sobre os quais, como referimos, o Grupo de Trabalho do Artigo 29.º aprovara o *Parecer 3/2012 sobre a evolução das tecnologias biométricas* e o CEPD, as *Diretrizes n.º 3/2019 relativas ao tratamento de dados pessoais através de sistemas de videovigilância* [videomonitoramento].

Porém, o mesmo "[…] não se aplica ao tratamento de dados pessoais: […] Efetuado pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública." (Art.º 2.º n.º 2 d)[11]-[12]

> [Na matéria, a *LGPD* dispõe que a mesma "[…] não se aplica ao tratamento de dados pessoais: III - realizado para fins exclusivos de: a) segurança pública; [ou] d) atividades de investigação e repressão de infrações penais; § 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.", Art. 4º; porém, mais de quatro anos depois, a referida lei está por aprovar, embora já existam Projetos com esse propósito; para um recente ponto da situação, a título apenas informativo, Maíra FERNANDES, Daniela MEGGIOLARO & Fernanda PRATES (2022), ademais de, incidindo especificamente sobre o nosso objeto, Eduarda Costa ALMEIDA (2023) e Fernando Andrade FERNANDES & Ana Paula Bougleux Andrade RESENDE (2023)]

[11] O que, em Portugal, afasta também a aplicação da Lei n.º 58/2019, de 8 de agosto, e das fontes legislativas especiais, cujo mapeamento fora realizado por Lurdes Dias ALVES (2019), salvo no que se refere à articulação com o então disposto na Lei n.º 1/2005, de 10 de janeiro, a qual regula a utilização de câmaras de vídeo pelas forças e serviços de segurança em locais públicos de utilização comum [entretanto abrogada e substituída pela Lei n.º 95/2021, de 29 de dezembro, a qual 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 [videomonitoramento] para captação, gravação e tratamento de imagem e som], embora a Autora não tenha estabelecido a ligação desta Lei com a *Diretiva LE*, indispensável desde a sua publicação, atendendo ao *Princípio da Interpretação Conforme ao Direito da União*, ou da *Aplicabilidade Indireta* das diretivas, enunciado pelo TJUE nos Acórdãos *von Colson e Kamann* (Processo C-14/83, de 10 de abril de 1984), *Murphy* (Processo C-157/86, de 4 de fevereiro de 1988) e *Marleasing* (Processo (C-106/89, de 13 de novembro de 1990, o mesmo podendo dizer-se a propósito do estudo de Inês Pereira de SOUSA (2018), inclusive explicando boa parte das perplexidades que o permeiam; anteriormente, a Lei n.º 1/2005 fora objeto de uma análise crítica por parte de Catarina FROIS (2011), incluindo a análise de casos, embora também sem atender ao tratamento de dados biométricos.

[12] Esta opção do Legislador europeu tem sido contestada por alguns, como Inês OLIVEIRA (2019), a qual propugna por uma unicidade da disciplina da Proteção de Dados. Porém, creio que essa alternativa não seria viável em atenção à diversidade dos Direitos Fundamentais postos em risco e das respostas institucionais a serem consideradas nos domínios da Segurança Pública e da Justiça Criminal, incluindo o Terrorismo, além de o Art.º 83.º do *TFUE – Tratado sobre o Funcionamento da União Europeia*, preterir os regulamento pelas diretivas em matéria penal, em atenção à respetiva delicadeza político-constitucional, como procurámos mostrar, Manuel David MASSENO (2021) e, sobretudo, (2022 [b]), tal como o fez Raquel A. Brízida Castro (2020). Adicionalmente, como aponta o *Considerando* (20) do *RGPD*, o tratamento de dados na Justiça, inclusivamente cível, requer regimes especiais, como resulta de José Joaquim MARTINS (2022), aliás em linha com o meu texto, indicado acima (2021).

Daí resulta a especial relevância da *Diretiva LE*[13]-[14], de acordo com a qual esse tratamento:

> "[…] só é autorizado se for estritamente necessário [*id est*, indo além do "necessário" para a sua licitude em termos gerais, Art.º 8.º n.º 1], se estiver sujeito a garantias adequadas dos direitos e liberdades do titular dos dados, e se [adicionalmente]: a) For autorizado pelo direito da União ou de um Estado-Membro; b) Se destinar a proteger os interesses vitais do titular dos dados ou de outra pessoa singular [natural]; ou c) Estiver relacionado com dados manifestamente tornados públicos pelo titular dos dados." (Art.º 10.º) [em termos ainda mais exigentes que o previsto pela *LGPD* para o "tratamento de dados pessoais sensíveis", Art. 11]

Adicionalmente, é imposta a observância estrita pelas "Autoridades competentes" dos Princípios da «licitude e lealdade», da «limitação das finalidades», da «exatidão», da «minimização dos dados», da «limitação da conservação» e, ainda, da «integridade e confidencialidade» (Art.º 4.º n.º 1, para usar a terminologia do RGPD, pois a Diretiva LE não os nomeia) e a garantia dos direitos à informação e de acesso, embora com limitações relativamente ao disposto no RGPD (Art.ºs 13.º, 14.º e 15.º) [em grande medida coincidentes com o disposto no Art. 6º da LGPD][15].

---

[13] A propósito desta, têm o maior interesse as *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*, do CEPD, de 12 de maio de 2022 / 26 de abril de 2023, ainda sem versão oficial em língua portuguesa, assim como o Relatório da FRA – Agência da União Europeia para os Direito Fundamentais "Facial recognition technology: fundamental rights considerations in the context of law enforcement", de 27 de novembro de 2019, apenas disponível também em alemão e em francês desde 1 de março de 2022; sem esquecer as referências, sintéticas mas muito pertinentes, que constam do *Parecer sobre algumas questões importantes da Diretiva relativa à proteção de dados na aplicação da lei (Diretiva (UE) 2016/680)*, 29 de novembro de 2017, ainda do Grupo de Trabalho do Artigo 29.º.

[14] Acrescente-se que a mesma qual foi transposta pela Lei n.º 59/2019, de 8 de agosto, [que] aprova 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, depois completada pela completada pela Lei n.º 95/2021, de 29 de dezembro, à qual aliás regressaremos.

[15] Preceitos estes explicitados nos *Considerando* (26), em cujos termos "O tratamento de dados pessoais tem de ser feito de forma lícita, leal e transparente para com as pessoas singulares [naturais] em causa, e exclusivamente para os efeitos específicos previstos na lei. Tal não obsta, em si mesmo, a que as autoridades de aplicação da lei exerçam atividades tais como investigações encobertas ou videovigilância [videomonitoramento]. Tais atividades podem ser executadas para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública, desde que estejam previstas na lei e constituam uma medida necessária e proporcionada numa sociedade democrática, tendo devidamente em conta os interesses legítimos da pessoa singular [natural] em causa. […] As pessoas singulares [naturais] deverão ser alertadas para os riscos, regras, garantias e direitos associados ao tratamento dos seus dados pessoais e para os meios de que dispõem para exercer os seus direitos relativamente ao tratamento desses dados. Em especial, os efeitos específicos do tratamento deverão ser explícitos e legítimos, e deverão estar determinados no momento da recolha dos dados pessoais. Os dados pessoais deverão ser adequados e relevantes para os efeitos para os quais são tratados. É especialmente necessário garantir que os dados pessoais recolhidos não sejam excessivos nem conservados durante mais tempo do que o necessário para os efeitos para os quais

Por seu turno, a «Definição de perfis» (Art.º 3.º 4) a partir do tratamento de tais dados, ao ter inerente um acréscimo dos "riscos para os direitos e liberdades das pessoas" está vedada, "[…] a não ser que sejam aplicadas medidas [adicionais] adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular" e, em qualquer caso, sempre que "conduzam à discriminação de pessoas singulares [naturais]" (Art.º 11.º n.ºs 2 e 3)[16], além de pressupor a realização duma AIPD/DPIA - "avaliação de impacto sobre proteção de dados" [um "relatório de impacto à proteção de dados pessoais", na definição do Artº 5º XVII da LGPD], ao ser, manifestamente, "suscetível de resultar num elevado risco para os direitos e liberdades das pessoas singulares [naturais]", inclusive por estarmos perante o tratamento de uma categoria especial de dados (Art.ºs 10.º e 27.º n.º 1)[17] [enquanto a LGPD prevê que "A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais.", no Art. 4º § 4º].

O mesmo se podendo dizer quanto à pertinência de uma "consulta prévia da autoridade de controlo", mesmo sem uma prévia avaliação de impacto, quando "O tipo de tratamento envolva, especialmente no caso de se utilizarem novas tecnologias, mecanismos ou procedimentos, um elevado risco para os direitos e liberdades dos titulares dos dados" (Art.º 28.º n.º 1 b).

são tratados. Os dados pessoais só deverão ser tratados se a finalidade do tratamento não puder ser atingida de forma razoável por outros meios. A fim de assegurar que os dados são conservados apenas durante o período considerado necessário, o responsável pelo tratamento deverá fixar prazos para o seu apagamento ou revisão periódica. Os Estados-Membros deverão prever garantias adequadas aplicáveis aos dados pessoais conservados durante períodos mais longos a fim de fazerem parte de arquivos de interesse público ou de serem utilizados para fins científicos, estatísticos ou históricos." da Diretiva *de qua*.

[16] No que se afasta do regime previsto pelo Art.º 22.º do *RGPD*, a propósito do qual remetemos para os nossos trabalhos anteriores, Manuel David MASSENO & Cristiana Teixeira SANTOS (2019), assim como para os estudos de posteriores de Beatriz Santiago TRINDADE (2020), de Inês SILVA COSTA (2021), de Pedro Miguel J. CORREIA (2022), de Maria Raquel GUIMARÃES (2022) e de Mafalda Miranda BARBOSA (2023), tendo por referência necessária as *Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679*, de 3 de outubro de 2017 / 6 de fevereiro de 2018, do Grupo de Trabalho do Artigo 29.º; assim como, no que se concerne à *Diretiva LE*, para Manuel David MASSENO (2022 [b]), além de para as referências breves de Raquel A. Brízida Castro (2020) e de Laura NEIVA (2020).

[17] Pela proximidade dos regimes, as *Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679*, do Grupo de Trabalho do Artigo 29.º, de 7 de abril / 4 de outubro de 2017, e as considerações a este propósito de Lurdes Dias ALVES (2019), de Bruno PEREIRA & João ORVALHO (2019) e bem assim as de Eliseu F. Pinto LOPES (2022), podem também servir de referência à elaboração de uma DPIA neste domínio, sempre que não percamos de vista a especificidades dos riscos relativamente aos direitos dos titulares dos dados, nas suas distintas categorias, além de distinguir "os dados pessoais baseados em factos" dos "dados pessoais baseados em apreciações pessoais" (Art.ºs 7.º e 6.º).

O que conduzirá à exigência de apenas serem utilizadas tecnologias que permitam discriminar o tratamento entre as categoriais previstas[18] e, no limite, só os de "pessoas relativamente às quais existem motivos fundados para crer que cometeram ou estão prestes a cometer [ou as já] condenadas por uma infração penal" (Art.º 6.º a) e b), distinguindo-as dos não suspeitos. Daí resultando ainda a interdição de utilizar outras bases de dados biométricos, em especial das criadas para finalidades distintas das da Segurança Pública e da Justiça Criminal.

3 – Tenteando o que estará para vir

Em finais de abril de 2021 e culminando trabalhos preparatórios específicos iniciados três anos antes, a Comissão Europeia avançou com uma *Proposta de Regulamento Inteligência Artificial*, com o objetivo explícito de garantir o "respeito pela dignidade humana" enquanto referência mor (Art.ºs 2.º do *TUE – Tratado da união Europeia* e 1.º da *CDFUE*)[19]

[18] Entre, "a) Pessoas relativamente às quais existem motivos fundados para crer que cometeram ou estão prestes a cometer uma infração penal; b) Pessoas condenadas por uma infração penal; c) Vítimas de uma infração penal ou pessoas relativamente às quais certos factos levam a crer que possam vir a ser vítimas de uma infração penal; e d) Terceiros envolvidos numa infração penal, tais como pessoas que possam ser chamadas a testemunhar em investigações penais relacionadas com infrações penais ou em processos penais subsequentes, pessoas que possam fornecer informações sobre infrações penais, ou contactos ou associados de uma das pessoas a que se referem as alíneas a) e b)" (Art.º 6.º), cujo sentido é sublinhado pelo *Considerando* (31), "Importa, portanto, estabelecer, se aplicável e tanto quanto possível, uma clara distinção entre dados pessoais de diferentes categorias de titulares de dados, tais como suspeitos, pessoas condenadas por um crime, vítimas e terceiros, designadamente testemunhas, pessoas que detenham informações ou contactos úteis, e os cúmplices de pessoas suspeitas ou condenadas. Tal não deverá impedir a aplicação do direito à presunção de inocência, tal como garantido pela Carta [*dos Direitos Fundamentais da União Europeia*] e pela CEDH [*Convenção Europeia dos Direitos Humanos e das Liberdades Fundamentais*, de 4 de novembro de 1950, ao qual a UE ficou habilitada a aderir pelo Art.º 6.º n.º 2 do *TUE*], de acordo com a interpretação da jurisprudência do Tribunal de Justiça e do Tribunal Europeu dos Direitos do Homem, respetivamente"; como, aliás, defendemos a propósito da "definição de perfis" no âmbito desta mesma *Diretiva*, Manuel David MASSENO (2022 [b]).

[19] Por extenso, a *Proposta de Regulamento que estabelece regras harmonizadas em matéria de Inteligência Artificial* (*Regulamento Inteligência Artificial*) (COM/2021/206 final, de 21 de abril de 2021), a par da contemporânea Comunicação da Comissão [Europeia] ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões, *Fomentar uma abordagem europeia da inteligência artificial* (COM(2021) 205 final), culminando um processo pré-legislativo envolvendo as Instituições e as Agências da UE. Sobre a Proposta, além da apresentação de Cristina CALDEIRA (2021) e da análise de teor geral de Tiago Sérgio CABRAL (2021), assim como das reflexões críticas de Vera Lúcia RAPOSO (2021), de Francisco C. Pacheco de ANDRADE (2022) e de Mafalda Miranda BARBOSA (2023), permito-me remeter para a minha contextualização dos trabalhos preparatórios, Manuel David MASSENO (2022 [a]), ademais de, inclusive atendendo a algumas vicissitudes posteriores e tendo por objeto questões parcialmente sobreponíveis às que nos ocupam, Manuel David MASSENO (2022 [b]) [Desde o Brasil, são interessantes as análises de Marcos EHRARDT Jr. & Milton Pereira França NETTO (2023) e de Everton MENENGOLA, Emerson GABARDO & Nacy Nelly GONZÁLEZ SANMIGUEL (2023)].

Em extrema síntese, a Proposta distingue entre as "práticas de inteligência artificial proibidas" (Art.º 5.º), os "sistemas de inteligência artificial de risco elevado" (Art.ºs 8.º a 51.º) e as "obrigações de transparência aplicáveis a determinados sistemas de inteligência artificial", para os de baixo risco (Art.º 52.º), além dos e risco mínimo, os quais ficarão foram do âmbito de aplicação do futuro Regulamento (Art.º 1.º).

De entre as "práticas de inteligência artificial proibidas", sendo até a objeto de uma disciplina mais detalhada e "matizada", consta:

> "A utilização de sistemas de identificação biométrica à distância em «tempo real» em espaços acessíveis ao público para efeitos de manutenção da ordem pública, salvo se essa utilização for estritamente necessária para alcançar um dos seguintes objetivos: i) a investigação seletiva de potenciais vítimas específicas de crimes, nomeadamente crianças desaparecidas, ii) a prevenção de uma ameaça específica, substancial e iminente à vida ou à segurança física de pessoas singulares [naturais] ou de um ataque terrorista, iii) a deteção, localização, identificação ou instauração de ação penal relativamente a um infrator ou suspeito de uma infração penal referida no artigo 2.º, n.º 2, da Decisão-Quadro 2002/584/JAI do Conselho [relativa ao mandado de detenção europeu] e punível no Estado-Membro em causa com pena ou medida de segurança privativas de liberdade de duração máxima não inferior a três anos e tal como definidas pela legislação desse Estado-Membro;" (Art.º 5.º n.º 1 d)

Porém, esta proibição é apenas relativa, ao estarem previstas diversas "exceções" e ser admitida e intervenção legislativa dos Estados-Membro, dispensando a intervenção

duma "autoridade judiciária [a qual poderá ser substituída] por uma autoridade administrativa independente"[2021].

Embora a própria Comissão esteja ciente, em termos manifestos e assumidos, que:

> "A utilização de sistemas de IA para a identificação biométrica à distância «em tempo real» de pessoas singulares [naturais] em espaços acessíveis ao público para efeitos de manutenção da ordem pública é considerada particularmente intrusiva para os direitos e as liberdades das pessoas em causa, visto que pode afetar a vida privada de uma grande parte da população, dar origem a uma sensação de vigilância constante e dissuadir indiretamente o exercício da liberdade de reunião e de outros direitos fundamentais. Além disso, dado o impacto imediato e as oportunidades limitadas para a realização de controlos adicionais ou correções da utilização desses sistemas que funcionam «em tempo real», estes dão origem a riscos acrescidos para os direitos e as liberdades das pessoas visadas pelas autoridades policiais

[20] Especificamente e em termos muito detalhados, "2.A utilização de sistemas de identificação biométrica à distância «em tempo real» em espaços acessíveis ao público para efeitos de manutenção da ordem pública que vise alcançar um dos objetivos referidos no n.º 1, alínea d), deve ter em conta os seguintes elementos: a) A natureza da situação que origina a possível utilização, em especial a gravidade, a probabilidade e a magnitude dos prejuízos causados na ausência da utilização do sistema; b) As consequências da utilização do sistema para os direitos e as liberdades de todas as pessoas afetadas, em especial a gravidade, a probabilidade e a magnitude dessas consequências. Além disso, a utilização de sistemas de identificação biométrica à distância «em tempo real» em espaços acessíveis ao público para efeitos de manutenção da ordem pública que vise alcançar um dos objetivos referidos no n.º 1, alínea d), deve observar salvaguardas e condições necessárias e proporcionadas em relação a tal utilização, nomeadamente no respeitante a limitações temporais, geográficas e das pessoas visadas. [Em termos adicionais,] 3. No tocante ao n.º 1, alínea d), e ao n.º 2, cada utilização específica de um sistema de identificação biométrica à distância «em tempo real» em espaços acessíveis ao público para efeitos de manutenção da ordem pública está sujeita a autorização prévia concedida por uma autoridade judiciária ou por uma autoridade administrativa independente do Estado-Membro no qual a utilização terá lugar após apresentação de um pedido fundamentado em conformidade com as regras de execução previstas no direito nacional a que se refere o n.º 4. Contudo, numa situação de urgência devidamente justificada, a utilização do sistema pode ser iniciada sem uma autorização e esta pode ser solicitada apenas durante ou após a utilização. A autoridade judiciária ou administrativa competente apenas deve conceder a autorização se considerar, com base em dados objetivos ou indícios claros que lhe tenham sido apresentados, que a utilização do sistema de identificação biométrica à distância «em tempo real» em apreço é necessária e proporcionada para alcançar um dos objetivos especificados no n.º 1, alínea d), conforme identificado no pedido. Ao decidir sobre o pedido, a autoridade judiciária ou administrativa competente tem em conta os elementos referidos no n.º 2. [e ainda] 4.Um Estado-Membro pode decidir prever a possibilidade de autorizar total ou parcialmente a utilização de sistemas de identificação biométrica à distância «em tempo real» em espaços acessíveis ao público para efeitos de manutenção da ordem pública dentro dos limites e sob as condições enumeradas no n.º 1, alínea d), e nos n.ºs 2 e 3. Esse Estado-Membro estabelece na sua legislação nacional as regras pormenorizadas aplicáveis ao pedido, à emissão e ao exercício das autorizações a que se refere o n.º 3, bem como à supervisão das mesmas. Essas regras especificam igualmente em relação a que objetivos enumerados no n.º 1, alínea d), incluindo quais das infrações penais referidas na subalínea iii) da mesma, as autoridades competentes podem ser autorizadas a usar esses sistemas para efeitos de manutenção da ordem pública."

[21] Sobre o conteúdo da Proposta, neste particular, criticamente, ainda que desde *loci* argumentativos díspares, são de atender as análises de Maria Raquel GUIMARÃES (2022), de Vera Lúcia RAPOSO (2022) e, ainda, de Rui Soares PEREIRA (2022).

Poucas semanas depois, em Parecer conjunto, o CEPD e a Autoridade Europeia para a Proteção de Dados concluíram que:

> "O raciocínio subjacente à proposta parece omitir que, ao vigiar áreas abertas, as obrigações ao abrigo da legislação da UE em matéria de proteção de dados têm de ser cumpridas não só para os suspeitos, mas também para todos aqueles que são objeto de vigilância na prática [e, adicionalmente] apelam à proibição geral de qualquer utilização de IA para o reconhecimento automatizado de características humanas em espaços acessíveis ao público (tal como de rostos, mas também do andar, de impressões digitais, do ADN, da voz, da digitação e de outros sinais comportamentais ou biométricos) em qualquer contexto"[22]

Ao passo que o Conselho Económico e Social Europeu foi muito crítico quanto à permissividade da *Proposta*[23] e o Comité das Regiões se preocupou essencialmente com os riscos inerentes à classificação social, passível de ser articulada com a identificação biométrica[24], enquanto o Banco Central Europeu nem opinou sobre esta[25].

A 6 de dezembro último, durante a Presidência checa e na sequência de negociações apenas passíveis de serem seguidas através dos Comunicados oficiais e das "filtrações" para a Imprensa, o Conselho de Ministros adotou uma *Orientação geral* sobre a *Proposta*, na sequência do acordo obtido no COREPER - Comité dos Representantes Permanentes a 25 de novembro (14954/22).

Na mesma, além de deixar de fora todas as utilizações de IA relacionadas com a segurança nacional e de "clarificar" os limites da proibição no que se refere à "identificação biométrica" para fins de prevenção e combate ao crime, com novas redações dos n.ºs 2, 3 e 4 do Art.º 5.º da *Proposta* da Comissão[26].

---

[22] O *Parecer conjunto 5/2021 do CEPD e da AEPD sobre a proposta de regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial (Regulamento Inteligência Artificial)*, de 18 de junho.

[23] No seu Parecer 2021/C 517/09, de 22 de setembro, até porque "A limitação da proibição à «manutenção da ordem pública» permite a identificação biométrica e todas as outras formas de reconhecimento biométrico que não visam identificar uma pessoa, incluindo todas as formas referidas de «reconhecimento de emoções», para todos os demais efeitos, por todos os demais intervenientes, em todos os lugares públicos e privados, incluindo no local de trabalho, nas lojas, nos estádios, nos teatros, etc., o que deixa a porta aberta a um mundo em que estamos constantemente sob «avaliação do ponto de vista emocional» para qualquer fim considerado necessário pelo interveniente que efetua essa avaliação.".

[24] Assim, o Parecer 2022/C 97/12, de 2 de dezembro de 2021.

[25] Como resulta do seu Parecer CON/2021/40, de 29 de dezembro, como até era espectável, em atenção às respetivas competências.

[26] Como justificado nos *Considerandos* (19) a (24), das "exceções" passou a constar, "2. A utilização de sistemas de identificação biométrica à distância "em tempo real" em espaços acessíveis ao público para efeitos de manutenção da ordem pública que vise alcançar um dos objetivos referidos no n.º 1, alínea d),

Por seu turno e intercalarmente, o Parlamento Europeu aprovou uma Resolução incluindo esta problemática, na qual defende um maior rigor no que se refere à disciplina do reconhecimento facial, incluindo uma moratória até à comprovação da robustez e precisão dos sistemas, salvo para a identificação de vítimas, e:

> "[…] apela, além disso, à proibição permanente do recurso a análises automatizadas e/ou do reconhecimento em espaços acessíveis ao público de outras características humanas, tais como o andar, as impressões digitais, o ADN, a voz e outros sinais biométricos e comportamentais."[27]

Entretanto, a 14 de junho de 2023, o Parlamento aprovou a sua *Posição comum em primeira leitura* (P9 TA(2023)0236). Da mesma consta uma alteração profunda à *Proposta*, reiterando as suas orientações de sempre, com a tónica a ser posta na garantia

deve ter em conta os seguintes elementos: a) A natureza da situação que origina a possível utilização, em especial a gravidade, a probabilidade e a magnitude dos prejuízos causados na ausência da utilização do sistema b) As consequências da utilização do sistema para os direitos e as liberdades de todas as pessoas afetadas, em especial a gravidade, a probabilidade e a magnitude dessas consequências. Além disso, a utilização de sistemas de identificação biométrica à distância "em tempo real" em espaços acessíveis ao público para efeitos de manutenção da ordem pública que vise alcançar um dos objetivos referidos no n.º 1, alínea d), deve observar salvaguardas e condições necessárias e proporcionadas em relação a tal utilização, nomeadamente no respeitante a limitações temporais, geográficas e das pessoas visadas."; ao que acrescenta o n.º 3, "No tocante ao n.º 1, alínea d), e ao n.º 2, cada utilização de um sistema de identificação biométrica à distância "em tempo real" em espaços acessíveis ao público para efeitos de manutenção da ordem pública está sujeita a autorização prévia concedida por uma autoridade judiciária ou por uma autoridade administrativa independente do Estado-Membro no qual a utilização terá lugar após apresentação de um pedido fundamentado em conformidade com as regras de execução previstas no direito nacional a que se refere o n.º 4. Contudo, numa situação de urgência devidamente justificada, a utilização do sistema pode ser iniciada sem uma autorização, desde que essa autorização seja solicitada sem demora injustificada durante a utilização do sistema de IA e, se essa autorização for rejeitada, a sua utilização seja suspensa com efeitos imediatos. A autoridade judiciária ou administrativa competente apenas deve conceder a autorização se considerar, com base em dados objetivos ou indícios claros que lhe tenham sido apresentados, que a utilização do sistema de identificação biométrica à distância "em tempo real" em apreço é necessária e proporcionada para alcançar um dos objetivos especificados no n.º 1, alínea d), conforme identificado no pedido. Ao decidir sobre o pedido, a autoridade judiciária ou administrativa competente tem em conta os elementos referidos no n.º 2."; porém, continua a prever que "4. Um Estado-Membro pode decidir prever a possibilidade de autorizar total ou parcialmente a utilização de sistemas de identificação biométrica à distância "em tempo real" em espaços acessíveis ao público para efeitos de manutenção da ordem pública dentro dos limites e sob as condições enumeradas no n.º 1, alínea d), e nos n.ºs 2 e 3. Esse Estado-Membro estabelece na sua legislação nacional as regras pormenorizadas aplicáveis ao pedido, à emissão e ao exercício das autorizações a que se refere o n.º 3, bem como à supervisão e comunicação das mesmas. Essas regras especificam igualmente em relação a que objetivos enumerados no n.º 1, alínea d), incluindo quais das infrações penais referidas na subalínea iii) da mesma, as autoridades competentes podem ser autorizadas a usar esses sistemas para efeitos de manutenção da ordem pública.".

[27] Especificamente, a Resolução do Parlamento Europeu, de 6 de outubro de 2021, sobre a inteligência artificial no direito penal e a sua utilização pelas autoridades policiais e judiciárias em casos penais (2020/2016(INI)).

das Liberdades e inerente afastamento da identificação biométrica "em tempo real", assim como da criação ou uso de bases de dados biométricos de âmbito geral[28].

Agora, falta-nos aguardar pelos resultados do trílogo interinstitucional. Mas, ainda assim, embora apenas enquanto *Softlaw*, podemos ter como parâmetro, pelo menos de natureza aspiracional, a *Declaração Europeia* [interinstitucional] *sobre os direitos e princípios digitais para a década digital* (2023/C), assinada pelos Presidentes do Parlamento Europeu, do Conselho e da Comissão, publicada oficialmente a 23 de janeiro de 2023.

[28] Em termos concreto, é introduzida uma modificação no *Considerando* (18), o qual passaria a ter por conteúdo que "A utilização de sistemas de IA para a identificação biométrica à distância «em tempo real» de pessoas singulares [naturais] em espaços acessíveis ao público é particularmente intrusiva para os direitos e as liberdades das pessoas em causa **e pode, em última análise**, afetar a vida privada de uma grande parte da população, dar origem a uma sensação de vigilância constante, **dar às partes que utilizam a identificação biométrica em espaços acessíveis ao público uma posição de poder incontrolável** e dissuadir indiretamente o exercício da liberdade de reunião e de outros direitos fundamentais **que estão no cerne do Estado de direito**. **As imprecisões técnicas dos sistemas de IA concebidos para a identificação biométrica à distância de pessoas singulares** [naturais] **podem conduzir a resultados enviesados e ter efeitos discriminatórios. Esta questão é particularmente relevante quando diz respeito à idade, à etnia, ao género ou a deficiências das pessoas**. Além disso, dado o impacto imediato e as oportunidades limitadas para a realização de controlos adicionais ou correções da utilização desses sistemas que funcionam «em tempo real», estes dão origem a riscos acrescidos para os direitos e as liberdades das pessoas visadas pelas autoridades policiais. **Como tal, deve ser proibida a utilização desses sistemas em locais acessíveis ao público. Do mesmo modo, os sistemas de IA utilizados para a análise de imagens registadas de espaços acessíveis ao público através de sistemas de pósidentificação biométrica à distância devem também ser proibidos, a menos que exista uma autorização judicial prévia para a sua utilização no contexto da aplicação da lei, quando estritamente necessária para a pesquisa direcionada ligada a uma infração penal grave e específica já ocorrida, e apenas mediante prévia autorização judicial**." (os negritos constam da fonte, correspondendo à redação introduzida), sendo em consequência suprimidos os *Considerandos* (19) a (23). No que se refere aos preceitos, além de inserir definições específicas no Art.º 3.º, como "(33-A) «Dados baseados em biometria», dados resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular [natural]", (33-B) «Identificação biométrica», o reconhecimento automatizado de características humanas físicas, fisiológicas, comportamentais e psicológicas para efeitos de determinação da identidade de uma pessoa, comparando os dados biométricos dessa pessoa com os dados biométricos de pessoas armazenados numa base de dados (identificação «um para muitos»);" e "(33-C) «Verificação biométrica», a verificação automatizada da identidade de pessoas singulares [naturais] através da comparação de dados biométricos de uma pessoa com dados biométricos previamente fornecidos (verificação «um para um», incluindo a autenticação);"; coerentemente com o enunciado na redação modificada dos *Considerandos*, entre as proibições previstas no Art.º 5.º n.º 1 passou a estar, em termos transversais, "d) A utilização de sistemas de identificação biométrica à distância em «tempo real» em espaços acessíveis ao público;"; ao passo que acrescenta novas alíneas ao Art.º 5.º 1.º, a d-B), em cujos termos, fica também proibida "A colocação no mercado, a colocação em serviço ou a utilização de sistemas de IA que criam ou expandem bases de dados de reconhecimento facial através da recolha aleatória de imagens faciais a partir da Internet ou de imagens de CCTV;" e "d-D) A colocação em serviço ou a utilização de sistemas de IA para a análise de vídeos de espaços acessíveis ao público através de sistemas de identificação biométrica à distância «em diferido», a menos que estejam sujeitos a uma autorização prejudicial em conformidade com a legislação da União e sejam estritamente necessários para a pesquisa precisa associada a uma infração penal grave específica, tal como definida no artigo 83.º, n.º 1, do TFUE, que já tenha ocorrido para efeitos de aplicação da lei.", suprimindo os n.ºs 2, 3 e 4.

Ora, esta, propósito das "Interações com algoritmos e sistemas de inteligência artificial", reitera que:

> "8. A inteligência artificial deve ser uma ferramenta ao serviço das pessoas e ter o objetivo último de aumentar o bem-estar dos seres humanos [e] 9. Todas as pessoas devem poder beneficiar das vantagens dos sistemas algorítmicos e dos sistemas de inteligência artificial, nomeadamente fazendo escolhas próprias e informadas no ambiente digital, estando simultaneamente protegidas contra os riscos e os danos para a saúde, a segurança e os direitos fundamentais."[29]

[Na sequência do *Relatório Final da Comissão de Juristas instituída pelo Ato do Presidente do Senado nº 4, de 2022, destinada a subsidiar a elaboração de minuta de substitutivo para instruir a apreciação dos Projetos de Lei nºs 5.051, de 2019, 21, de 2020, e 872, de 2021, que têm como objetivo estabelecer princípios, regras, diretrizes e fundamentos para regular o desenvolvimento e a aplicação da inteligência artificial no Brasil*, de dezembro de 2022, o Presidente do Senado e do Congresso Nacional, Rodrigo Pacheco (PSD/MG), apresentou Projeto de Lei n° 2338, 8 de maio de 2023, no qual está prevista uma disciplina relativa ao "uso de sistemas de identificação biométrica à distância", no respetivo Art. 15; enquanto na Câmara dos Deputados tramita o Projeto de Lei 3069/22, apresentado pelo Deputado Subtenente Gonzaga (PSD/MG), a 21 de dezembro de 2022, o qual *regulamenta o uso do reconhecimento facial automatizado pelas forças de segurança pública em investigações criminais ou procedimentos administrativos*; cumprindo seguir os respetivos desenvolvimentos em sede parlamentar; sobre o processo legislativo anterior ao *Relatório*, por todos, são de atender as considerações críticas de Marcos EHRARDT Jr. & Milton Pereira França NETTO (2023)]

[29] Daí o preceito acrescentar, programaticamente e com as consequências efetivas que vierem a ser positivadas, o seguinte: "Comprometemo-nos a: a) Promover sistemas de inteligência artificial centrados no ser humano, fiáveis e éticos ao longo do seu desenvolvimento, implantação e utilização, em consonância com os valores da UE; b) Assegurar um nível adequado de transparência sobre a utilização de algoritmos e inteligência artificial e a garantir que as pessoas sejam capacitadas para a sua utilização e informadas quando interagem com eles; c) Garantir que os sistemas algorítmicos se baseiam em conjuntos de dados adequados para evitar a discriminação e permitir a supervisão humana de todos os resultados que afetam a segurança e os direitos fundamentais das pessoas; […]; e) Prever salvaguardas e tomar medidas adequadas, nomeadamente através da promoção de normas fiáveis, para assegurar que a inteligência artificial e os sistemas digitais são sempre seguros e utilizados no pleno respeito dos direitos fundamentais; […].".

E, a modo de apêndice…

Ainda que venha a prevalecer a posição do Conselho no trílogo, é expectável a continuidade de uma margem, relativamente ampla, para os Legisladores nacionais na matéria.

Em Portugal e de momento, vigora a Lei n.º 95/2021, a qual 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 [videomonitoramento] para captação, gravação e tratamento de imagem e som, revogando a Lei n.º 1/2005, de 10 de janeiro. Ora, da mesma consta que

> para "os fins previstos do artigo 3.º [*i.e.*, os constantes da "Lei de Segurança Interna, aprovada pela Lei n.º 53/2008, de 29 de agosto, e em concreto **para**: [n.º 1] d) **Proteção da segurança das pessoas, animais e bens, em locais públicos ou de acesso público, e a prevenção da prática de factos qualificados pela lei como crimes, em locais em que exista razoável risco da sua ocorrência**; [incluindo a], e) **Prevenção de atos terroristas**;], o tratamento dos dados pode ter subjacente um sistema de gestão analítica dos dados captados, por aplicação de critérios técnicos [*i.e.*, através de IA, o que é deveras preocupante ao possibilitar a "definição de perfis", nos termos do Art.º 11.º da Lei n.º 59/2019, de 8 de agosto, a qual será legítima sempre que uma lei o preveja, mas necessitará sempre de uma leitura congruente com a *Constituição da República* e a *CDFUE*], de acordo com os fins a que os sistemas se destinam [mas] **não é permitida a captação e tratamento de dados biométricos**." (Art.º 16.º, n.ºs 1 e 2, sendo nossos os negritos)[30].

Referências:

ALVES, Lurdes Dias (2019. A videovigilância e a compressão da privacidade. *Anuário da Proteção de Dados - 2019*, pp. 138-155. Disponível em https://protecaodedadosue.cedis.fd.unl.pt/wp-content/uploads/2022/10/6.-Lurdes-Dias-Alves.pdf

ANDRADE, Francisco C. Pacheco de (2022). Análise crítica de alguns aspetos da Proposta de Regulamento Europeu para a Inteligência Artificial. *In*: SILVA, Eva Sónia Moreira da & FREITAS, Pedro Miguel (Eds.) *Inteligência artificial e robótica: desafios para o direito do século XXI*. Coimbra: GESTLEGAL, pp. 329-337. Disponível em https://gestlegal.pt/loja/inteligencia-artificial-e-robotica-desafios-para-o-direito-do-seculo-xxi/

[30] Sobre este regime, são de atender às reflexões de Maria Raquel GUIMARÃES (2022), sobretudo incidindo sobre os correspondentes trabalhos preparatórios.

BARBOSA, Mafalda Miranda (2023). Proteção de dados e inteligência artificial (também a propósito do *ChatGPT*). *Revista de Direito Comercial*, pp. 753-802. Disponível em https://www.revistadedireitocomercial.com/protecao-de-dados-e-inteligencia-artificial

CABRAL, Tiago Sérgio (2021). A proposta de Regulamento sobre Inteligência Artificial na União Europeia: uma breve análise. *In*: ABREU, Joana Covelo de; COELHO, Larissa & CABRAL, Tiago Sérgio (Eds.) *O Contencioso da União Europeia e a cobrança transfronteiriça de créditos: compreendendo as soluções digitais à luz do paradigma da Justiça eletrónica europeia (e-Justice)* – Vol. II. Braga: Pensamento Sábio - Associação para o conhecimento e inovação da Universidade do Minho / Escola de Direito, pp. 117-130. Disponível em https://repositorium.sdum.uminho.pt/bitstream/1822/73489/3/Contencioso%20da%20Uniao%20Europeia_eUjust_Vol%20II.pdf

CALDEIRA, Cristina M.ª de Gouveia (2021). Regulamento Inteligência Artificial. *Privacy and Data Protection Magazine* **2**, pp. 164-167. Disponível em https://www.europeia.pt/resources/media/documents/Revista_Privacy_and_Data_Protection_Magazine_N2.pdf

CASTRO, Raquel A. Brízida (2020). Proteção de Dados e a Diretiva EU 2016/680: o tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais. *In*: *Cibercriminalidade e Prova Digital*. Lisboa: Centro de Estudos Judiciários, 2018 (Atualizado em 2020), pp. 11-15. Disponível em https://cej.justica.gov.pt/LinkClick.aspx?fileticket=RH98QGW6e-U%3d&portalid=30

CORREIA, Sérgio Miguel J. (2022). O Direito de Oposição à Definição de Perfis. *Anuário da Proteção de Dados - 2022*, pp. 189-215. Disponível em https://protecaodedadosue.cedis.fd.unl.pt/wp-content/uploads/2022/12/6.-Sergio-Correia.pdf

COSTA, Inês Silva (2021). A proteção da pessoa na era dos *big data*: a opacidade do algoritmo e as decisões automatizadas. *RED – Revista Electrónica de Direito* **24** (1), pp. 33-82. Disponível em https://cij.up.pt//client/files/0000000001/4-ines-costa_1677.pdf

FONTES, José. O hexágono da prevenção criminal - A recolocação das medidas de polícia numa possível reconstrução das fronteiras da prevenção e repressão criminal (2022). *In*: MONTE, Mário Ferreira; LOUREIRO, Flávia Noversa & MORAIS, Pedro Jacob (Eds.) *I Congresso Internacional JusCrim "Prevenção, Policiamento e Segurança – Implicações nos Direitos Humanos"*. Braga: Escola de Direito da Universidade do Minho e Centro de Investigação em Justiça e Governação – JusCrim (Justiça Criminal e Criminologia), pp. 91-112. Disponível em https://repositorium.sdum.uminho.pt/bitstream/1822/80779/1/Atas_I_CI_JusCrim_2022_v2.pdf

FROIS, Catarina (2011). Video Surveillance in Portugal: Political Rhetoric at the Center of a Technological Project. *Social Analysis* 55 (3), pp. 35-53. Disponível em https://www.researchgate.net/publication/272212508_Video_SurVeillance_in_Portugal_Political_Rhetoric_at_the_Center_of_a_Technological_Project

_____ (2014). Video-surveillance and the Political Use of Discretionary Power in the Name of Security and Defence. *In*: MAGUIRE, Mark; FROIS, Catarina & ZURAWSKI, Nils (Eds.) *The Anthropology of Security Perspectives from the Frontline of Policing, Counter-terrorism and Border Control*. London: Pluto Press, pp. 45-61. Disponível em https://library.oapen.org/bitstream/handle/20.500.12657/54125/external_content.pdf

GUIMARÃES, Maria Raquel (2022). Inteligência artificial, *profiling* e direitos de personalidade. *In*: SILVA, Eva Sónia Moreira da & FREITAS, Pedro Miguel (Eds.) *Inteligência artificial e robótica: desafios para o direito do século XXI*. Coimbra: GESTLEGAL, pp. 187-211. Disponível em https://gestlegal.pt/loja/inteligencia-artificial-e-robotica-desafios-para-o-direito-do-seculo-xxi/

LOPES, Eliseu F. Pinto (2022). Avaliação de impacto sobre a proteção de dados. *Privacy and Data Protection Magazine* **5**, pp. 101-142. Disponível em https://bo.europeia.pt/content/files/pdpm_00598.pdf

MARTINS, José Joaquim (2022). Proteção de Dados e o Sistema Judicial Português – Uma síntese. *In*: BARZOTTO, Luciane Cardoso & COSTA, Ricardo Hofmeister de Almeida Martins (Eds.) *Estudos sobre LGPD – Lei Geral de Proteção de Dados – lei nº 13.709/2018: doutrina e aplicabilidade no âmbito laboral*. Porto Alegre: Escola Judicial do Tribunal Regional do Trabalho da 4ª Região / Diadorim Editora, pp. 112-128 Disponível em https://cdea.tche.br/site/wp-content/uploads/2022/05/Estudos-sobre-LGPD.pdf

MASSENO, Manuel David (2021). A segurança no tratamento de dados no sistema judicial, em Portugal e no Brasil. *Revista do CEJUR/TJSC: Prestação Jurisdicional* **9** (1). Disponível em https://revistadocejur.tjsc.jus.br/cejur/article/view/367

_____ (2022 [a]). Consideraciones breves sobre los Fundamentos de la Propuesta de Ley de Inteligencia Artificial de la Comisión Europea. *Journal of Law and Sustainable Development* **10** (1). Disponível em https://ojs.journalsdg.org/jlss/article/view/238

_____ (2022 [b]). La inteligencia artificial y la protección de datos: la "elaboración de perfiles" para la prevención de delitos graves y del terrorismo en las fuentes de la Unión Europea. *Revista Eletrônica do Curso de Direito da UFSM* **17** (2). Disponível em https://periodicos.ufsm.br/revistadireito/article/view/83679/60688

MASSENO, Manuel David & SANTOS, Cristiana Teixeira (2018 [a]). Cristiana Teixeira (2018 [a]). Between footprints: balancing environmental sustainability and privacy in smart tourism destinations. *Revista Eletrônica do Curso de Direito da UFSM* **13** (1), pp. 411-435. Disponível em https://periodicos.ufsm.br/revistadireito/article/view/32343

_____ (2018 [b]). Assuring Privacy and Data Protection within the Framework of Smart Tourism Destinations. *MediaLaws – Rivista di diritto dei media* **2**, pp. 251-266. Disponível em http://www.medialaws.eu/rivista/assuring-privacy-and-data-protection-within-the-framework-of-smart-tourism-destinations/

_____ (2019). Personalization and Profiling of Tourists in Smart Tourism Destinations – a Data Protection perspective. *Revista Argumentum* **20** (3), pp. 1215-1240. Disponível em http://ojs.unimar.br/index.php/revistaargumentum/article/view/1243

MOREIRA, Teresa Coelho & ANDRADE, Francisco C. Pacheco de (2016). Personal data and surveillance: the danger of the 'Homo Conectus'. *In*: NOVAIS, Paulo & KONOMI, Shin'ichi (Eds.). *Intelligent Environments - 2016*. Amsterdam: IOS Press, pp. 115-124. Disponível em http://ebooks.iospress.nl/volumearticle/45165

NEIVA, Laura (2020). *Big data na investigação criminal: desafios e expectativas na União Europeia*. Vila Nova de Famalicão: Húmus. Disponível em https://repositorium.sdum.uminho.pt/bitstream/1822/67004/1/BigDataInvCriminal_UE.pdf

OLIVEIRA, Inês (2019). Os regimes especiais de proteção de dados pessoais: exemplos de poluição legislativa da União Europeia? *Anuário da Proteção de Dados - 2019*, pp. 157-172. Disponível em https://protecaodedadosue.cedis.fd.unl.pt/wp-content/uploads/2022/10/7.-Ines-Oliveira.pdf

PEREIRA, Bruno; ORVALHO, João (2019). Avaliação de Impacto sobre a Protecção de Dados. *Cyberlaw by CIJIC* **7**. Disponível em https://www.iuris.edu.pt/xms/files/Cyberlaw-by-CIJIC_7.pdf

PEREIRA, Rui Soares (2022). Sobre o uso de sistemas de identificação biométrica (e de tecnologias de reconhecimento facial) para fins de segurança pública e de aplicação coerciva da lei: reflexões a propósito do da proposta de regulamento europeu sobre a inteligência artificial. *Revista da Faculdade de Direito da Universidade de Lisboa* **63** (1/2), pp. 839-865. Disponível em https://www.fd.ulisboa.pt/wp-content/uploads/2022/12/Rui-Soares-Pereira.pdf

RAMALHO, David Silva & COIMBRA, José Duarte (2015). A declaração de invalidade da Directiva 2006/24/CE: presente e futuro da conservação de dados de tráfego. *O Direito* **147** (IV), pp. 997-1045. Disponível em https://www.academia.edu/31146175/A_declara%C3%A7%C3%A3o_de_invalidade_da_Directiva_2006_24_CE_presente_e_futuro_da_conserva%C3%A7%C3%A3o_de_dados_de_tr%C3%A1fego

RAPOSO, Vera Lúcia (2021). Proposta de Regulamento sobre a Inteligência Artificial: *The devil is in the detais*. *Privacy and Data Protection Magazine* **3**, pp. 9-24. Disponível em https://www.europeia.pt/resources/media/documents/Revista_Privacy_and_Data_Protection_Magazine_N3.pdf

_____ (2022). The Use of Facial Recognition Technology by Law Enforcement in Europe: a Non-Orwellian Draft Proposal. *European Journal on Criminal Policy and Research*. Disponível em https://link.springer.com/article/10.1007/s10610-022-09512-y

SILVEIRA, Alessandra & FREITAS, Pedro Miguel (2017). Implicações da declaração de invalidade da Diretiva 2006/24 na conservação de dados ("metadados") nos Estados-Membros da UE: uma leitura jusfundamental. *Revista de Direito, Estado e Telecomunicações* **9** (1), pp. 47-68. Disponível em https://periodicos.unb.br/index.php/RDET/article/view/21513

SOUSA, Inês Pereira de (2018). No respeito pela vida (relativamente) privada no âmbito da videovigilância. *Fórum de Proteção de Dados* **5**, pp. 60-73. Disponível em https://www.cnpd.pt/media/qyzo5e4c/forum5_af_web_low.pdf

TORRES, Manuel Poêjo & DANTAS, Afonso de Freitas (2020). State Surveillance: How is Face Recognition Technology Impacting in the Political-Juridical Landscape? *Cyberlaw by CIJIC* **10**, pp. 123-156. Disponível em https://www.iuris.edu.pt/xms/files/Cyberlaw-by-CIJIC_10.pdf

TRINDADE, Beatriz Santiago (2020). Two years in: Does the GDPR already need updates? *A question brought by algorithmic decision-making*. *Anuário da Proteção de Dados - 2020*, pp. 79-103. Disponível em https://protecaodedadosue.cedis.fd.unl.pt/wp-content/uploads/2022/10/3.-Beatriz-Santiago-Trindade.pdf

VAZ, Ana (2007). Segurança da Informação, Protecção da Privacidade e dos Dados Pessoais. *Nação e Defesa* **117**, pp. 35-63. Disponível em https://comum.rcaap.pt/bitstream/10400.26/1218/1/NeD117_AnaVaz.pdf

VILAÇA, José L. da Cruz (2019). The digital world and the new frontiers of the European courts caselaw. *UNIO – EU Law Journal* **4** (1), pp. 4-15. Disponível em https://revistas.uminho.pt/index.php/unio/article/download/247/247/476

[**Referências adicionais**

ARRUDA, Ana Julia Pozzi; RESENDE, Ana Paula Bougleux Andrade & FERNANDES, Fernando Andrade (2021). Sistemas de policiamento preditivo e de afetação dos direitos humanos à luz da criminologia crítica. *Revista Direito Público* **18** (100). Disponível em https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/5978

COSTA, Ramon Silva & KREMER, Bianca (2022). Inteligência artificial e discriminação: desafios e perspectivas para a proteção de grupos vulneráveis frente às tecnologias de reconhecimento facial. *Revista Brasileira de Direitos Fundamentais & Justiça* **16** (1). Disponível em https://dfj.emnuvens.com.br/dfj/article/view/1316

EHRARDT Jr., Marcos & NETTO, Milton Pereira França (2023). O marco regulatório da Inteligência Artificial no Brasil: Entre avanços e retrocessos (2023). *JURISMAT* **16**, pp. 143-162. Disponível em https://revistas.ulusofona.pt/index.php/jurismat/article/view/8857

FERNANDES, Fernando Andrade & RESENDE, Ana Paula Bougleux Andrade. Regulamentação do tratamento automatizado de dados pessoais em matéria penal (2023). *Suprema - Revista de Estudos Constitucionais* **3** (1), pp. 471-500. Disponível em https://suprema.stf.jus.br/index.php/suprema/article/view/207]

FERNANDES, Maíra; MEGGIOLARO, Daniela & PRATES, Fernanda (2022). Lei de Proteção de Dados para segurança pública e persecução penal. *Consultor Jurídico*, 28 out. 2022. Disponível em: https://www.conjur.com.br/2022-out-28/escritos-mulher-lei-protecao-dados-seguranca-publica-persecucao-penal

FRANCISCO, Pedro Augusto; HUREL, Louise Marie & RIELLI, Mariana Marques (2020). *Regulação do reconhecimento facial no setor público: avaliação de experiências internacionais*. Rio de Janeiro: Instituto Igarapé. Disponível em: https://igarape.org.br/wp-content/uploads/2020/06/2020-06-09-Regula%C3%A7%C3%A3o-do-reconhecimento-facial-no-setor-p%C3%BAblico.pdf

MELO, Paulo Victor & SERRA, Paulo (2022). Tecnologia de Reconhecimento Facial e Segurança Pública nas Capitais Brasileiras: Apontamentos e Problematizações. *Comunicação e Sociedade* **42**, pp. 205-2020. Disponível em https://journals.openedition.org/cs/8111

MENENGOLA, Everton; GABARDO, Emerson & GONZÁLEZ SANMIGUEL, Nancy Nelly (2023). A proposta europeia de regulação da inteligência artificial. *Seqüência: Estudos Jurídicos Políticos* **43** (91), pp. 1–27. Disponível em https://periodicos.ufsc.br/index.php/sequencia/article/view/91435

MOZETIC, Vinícius de Almada & BARBIERO, Diego Roberto (2022). *Surveillance* e a Teoria da Ponderação: o conflito entre o direito à privacidade e a segurança pública no Brasil. *Revista Argumentum* **23** (1). Disponível em http://ojs.unimar.br/index.php/revistaargumentum/article/view/1268

PINTO, Fernanda Miler Lima (2023). Apontamentos sobre o caso do reconhecimento fácil a partir de videomonitoramento em vias públicas para fins penais no Brasil. *Revista Campo da História* **8** (1), pp. 308-318. Disponível em https://ojs.campodahistoria.com.br/ojs/index.php/rcdh/article/view/102

SCHNEIDER, Camila Berlim & MIRANDA, Pedro Fauth Manhães (2019). Vigilância digital como instrumento de promoção da segurança pública. *Publicatio UEPG: Ciências Sociais Aplicadas* **28**, pp. 1-14. Disponível em https://revistas.uepg.br/index.php/sociais/article/view/14435

SILVA, Rosane Leal da & SILVA, Fernanda dos Santos Rodrigues da (2019). Reconhecimento facial e segurança pública: os perigos do uso da tecnologia no sistema penal seletivo brasileiro. In: *Anais do 5º Congresso Internacional de Direito e Contemporaneidade: mídias e direitos da sociedade em rede*. Santa Maria: Universidade Federal de Santa Maria / Centro de Ciências Sociais e Humanas. Disponível em https://www.ufsm.br/app/uploads/sites/563/2019/09/5.23.pdf

VARGAS, Érica Nascimento Pinheiro & Mônica Matos RIBEIRO (2023). A Sociedade do Controle Digital e a Segurança Pública Brasileira. *Revista Direito UNIFACS – Debate Virtual* **277**, pp. 1-24. Disponível em https://revistas.unifacs.br/index.php/redu/article/view/8297

As hiperconexões foram verificadas no dia 14 de julho de 2023.