REVISTA DA FACULDADE DE DIREITO DA UNIVERSIDADE DE LISBOA

LISBON LAW REVIEW

Número Temático: Tecnologia e Direito

ANO LXIII 2022 NÚMEROS 1 E 2

REVISTA DA FACULDADE DE DIREITO
DA UNIVERSIDADE DE LISBOA
Periodicidade Semestral
Vol. LXIII (2022) 1 e 2

LISBON LAW REVIEW

PROPRIEDADE E SECRETARIADO

Faculdade de Direito da Universidade de Lisboa
Alameda da Universidade – 1649-014 Lisboa – Portugal

EDIÇÃO, EXECUÇÃO GRÁFICA E DISTRIBUIÇÃO
LISBON LAW EDITIONS

Alameda da Universidade – Cidade Universitária – 1649-014 Lisboa – Portugal

ISSN 0870-3116 Depósito Legal n.º 75611/95

Data: Outubro, 2022

ÍNDICE 2022

LIVROS & ARTIGOS

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 da proposta de regulamento europeu sobre a inteligência artificial

On the use of biometric data systems (and facial recognition technologies) for security and law enforcement purposes: reflections on the proposal for the european regulation on artificial intelligence

Rui Soares Pereira*

Resumo: Os sistemas de identificação biométrica, incluindo aplicativos ou tecnologias de reconhecimento facial, podem ser úteis para fins de verificação, identificação e categorização por parte de agentes públicos ou privados. Diversas vantagens e desvantagens têm sido identificadas quanto ao uso de sistemas de reconhecimento facial, as quais precisam de ser enfrentadas. A Proposta de Regulamento Europeu sobre a Inteligência Artificial, apresentada pela Comissão em 21 de abril de 2021, inclui novas e importantes regras na matéria. Adotando uma abordagem restritiva, representa um avanço significativo na regulamentação do uso na União Europeia de sistemas de identificação biométrica em geral e das tecnologias de reconhecimento facial também para fins de segurança pública e de aplicação coerciva

Abstract: Biometric data systems, including facial recognition applications or technologies, may be useful for verification, identification, and categorization purposes by public or private actors. Several advantages and disadvantages have been identified regarding the use of facial recognition systems, which need to be addressed. The draft EU Artificial Intelligence (AI) act, unveiled by the Commission on April 21st, 2021, has included new and important rules on the matter. While adopting a restrictive approach, represents a major step forward for regulating the use in the European Union of biometric data systems in general and facial recognition technologies also for security and law enforcement purposes. The Proposal seeks to be aligned with other European legal frameworks and requirements

* Professor Auxiliar da Faculdade de Direito da Universidade de Lisboa; ruisoarespereira@fd.ulisboa.pt.

da lei. A Proposta procura estar alinhada com outros regimes e requisitos jurídicos europeus e, se assim for, poderá ser vista como uma fonte de inspiração para outros países e jurisdições que pretendam aprovar legislação abrangente na matéria, a qual poderia permitir o uso (embora de forma restritiva) de tecnologias de reconhecimento facial automático pelas autoridades policiais e a sua inclusão no sistema de justiça penal.

Palavras-chave: Sistemas de identificação biométrica; tecnologias de reconhecimento facial; regulamentação de sistemas de identificação biométrica; Proposta de Regulamento Europeu sobre a Inteligência Artificial; fins de segurança pública e de aplicação coerciva da lei.

and, if so, it may be seen as a source of inspiration for other countries and jurisdictions who may wish to enact comprehensive legislation on the matter, which would allow the use (albeit in a restrictive way) of automated facial recognition technologies by law enforcement authorities and its inclusion in the criminal justice system.

Keywords: Biometric data systems; facial recognition technologies; regulation of biometric data systems; Proposal for the EU Regulation on Artificial Intelligence; security and law enforcement purposes.

1. Introdução

I. A Proposta de Regulamento Europeu sobre a Inteligência Artificial, apresentada pela Comissão em 21 de abril de 2021[1], tem diversas implicações em matéria de segurança.

Uma dessas implicações diz respeito às discussões acerca do uso de sistemas de identificação biométrica e tecnologias de reconhecimento facial para fins de segurança pública e de aplicação coerciva da lei.

Este importante tema é especificamente enfrentado, não apenas pela Proposta de Regulamento Europeu sobre a Inteligência Artificial, mas também por outros relevantes regimes jurídicos europeus. A Carta de Direitos Fundamentais, o Regulamento Geral de Proteção de Dados (doravante, RGPD), a Resolução do Parlamento Europeu sobre a inteligência artificial no direito penal e a sua utilização pelas autoridades policiais e judiciárias em casos penais (2020/2016(INI))[2] e o regime europeu de não discriminação incluíram já regras rígidas quanto à utilização de sistemas de identificação biométrica.

Não obstante, uma vez que a efetividade do atual quadro normativo da União Europeia sobre o tema dos sistemas de identificação biométrica (e tecnologias de reconhecimento facial) foi posta em causa por vários autores, a Proposta apresentada pela Comissão, e tornada pública em 21 de abril de 2021, estabeleceu várias outras normas para limitar a utilização de sistemas de identificação biométrica na União Europeia, incluindo tecnologias de reconhecimento facial. A preocupação central é a de evitar que esses sistemas e tecnologias possam conduzir àquilo que tem sido designado como "vigilância omnipresente" ("*ubiquitous surveillance*") na União Europeia[3].

II. A estratégia incluída na Proposta do Regulamento Europeu nesta matéria, apesar de não excluir *in totum* a utilização de sistemas de identificação biométrica,

---

[1] Proposta de Regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial (Regulamento Inteligência Artificial) e altera determinados atos legislativos da União, COM(2021) 206 final, disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52021PC0206&from=EN.

[2] Iniciativa apresentada em 2020 (disponível em https://www.europarl.europa.eu/doceo/document/LIBE-PR-652625_PT.pdf), aprovada em 6 de outubro de 2021 e publicada no Jornal Oficial da União Europeia em 24 de março de 2022 (disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52021IP0405&from=PT).

[3] Tambiama Madiega / Hendrik Mildebrath, *Regulating facial recognition in the EU*, EPRS | European Parliamentary Research Service, September 2021, p. I.

parece ser bastante mais restritiva do que as abordagens encontradas noutros países e jurisdições.

Não apenas se compararmos o quadro jurídico europeu com o caso da China (um dos primeiros países a fazer uso de tecnologias de reconhecimento facial para diversas e discutíveis finalidades)[4] ou se compararmos com a situação dos EUA em que se assistiu a uma rápida evolução da utilização da tecnologia de reconhecimento facial. Além disso, o uso de sistemas de identificação biométrica, tais como tecnologias de reconhecimento facial, constitui uma realidade em diversos outros países e a expansão do seu uso no futuro, para fins de segurança pública e de aplicação coerciva da lei, é (ou deveria ser) amplamente discutida.

III. O presente artigo visa identificar os aspetos fundamentais da estratégia da União Europeia no que respeita ao uso de sistemas de identificação biométrica e tecnologias de reconhecimento facial para fins de segurança pública e aplicação coerciva da lei e também comparar a regulamentação da União Europeia nesta matéria com a regulamentação existente noutros países e jurisdições.

A sequência do artigo é a seguinte:

Em primeiro lugar, faremos uma breve explicação da utilização de sistemas de identificação biométrica e de tecnologias de reconhecimento facial para fins policiais (2.).

Em segundo lugar, apresentaremos um esboço breve das preocupações principais quanto ao uso de sistemas de identificação biométrica mesmo para fins de segurança pública e aplicação coerciva da lei (3.).

Em terceiro lugar, faremos referências às experiências de outros países e jurisdições no que respeita ao uso e regulamentação de sistemas de identificação biométrica e de tecnologias de reconhecimento facial para fins de segurança pública e aplicação coerciva da lei (4.).

Em quarto lugar, apresentaremos os aspetos fundamentais da estratégia da União Europeia para a Inteligência Artificial e para os sistemas de identificação biométrica (5.).

No final, faremos algumas considerações finais, incluindo uma sintética avaliação da Proposta da Comissão, e concluiremos que, comprovando-se o alinhamento da Proposta com outros regimes e requisitos jurídicos europeus, a mesma poderá ser vista como uma fonte de inspiração para outros países e jurisdições que

[4] Por exemplo, foi recentemente difundida a existência de vigilância através de reconhecimento facial visando jornalistas – https://www.welt.de/newsticker/dpa_nt/infoline_nt/netzwelt/article235365936/Ueberwachung-mit-Gesichtserkennung-in-China-auch-fuer-Reporter.html.

pretendam aprovar legislação (ainda que de uma forma restritiva) nesta matéria (6.).

2. O uso de sistemas de identificação biométrica (e de tecnologias de reconhecimento facial) para fins policiais

2.1. As características dos sistemas de identificação biométrica e das tecnologias de reconhecimento facial

I. Podemos começar por caracterizar os sistemas de identificação biométrica e as tecnologias de reconhecimento facial.

Em síntese, os sistemas de identificação biométrica operam à distância sem que se saiba de antemão se a pessoa relevante estará presente numa certa área, recolhem dados biométricos (incluindo através do reconhecimento da imagem facial), comparam esses dados com uma amostra existente ou com uma base de dados sem atraso significativo e são usados especificamente para identificar um indivíduo.

Com as tecnologias de reconhecimento facial torna-se possível usar uma base de dados de imagens e vídeos, tais como a dos cartões de identificação, das cartas de condução, das câmeras de segurança, das imagens de cartões da escola e de outras bases de dados, para identificar pessoas na vida real ou em filmes e imagens de segurança.

II. O facto de os sistemas de identificação biométrica e de reconhecimento facial possuírem estas características torna-os ferramentas muito interessantes para agentes públicos e privados[5].

Em virtude da sua componente de vigilância e controle, as tecnologias de reconhecimento facial têm um vasto campo de aplicação, incluindo centros comerciais, aeroportos, estádios, concertos e controlo policial. A tecnologia de reconhecimento facial possui também o potencial de prevenir o crime, identificar criminosos, encontrar crianças perdidas e apoiar outros objetivos de segurança nacional. Por assim ser, não deve constituir surpresa que (também) as autoridades policiais estejam profundamente interessadas em usar tais sistemas.

---

[5] Sublinhando esse aspeto em relação às tecnologias de reconhecimento facial, cfr. Vera Lúcia Raposo, "(Do not) remember my face: uses of facial recognition technology in light of the general data protection regulation", in *Information & Communications Technology Law*, 2022, disponível em https://doi.org/10.1080/13600834.2022.2054076.

2.2. A distinção entre a segurança pública e a atividade de perseguição criminal

A utilização de sistemas de identificação biométrica (e de tecnologias de reconhecimento facial) para fins policiais é habitualmente discutida em relação à atividade que o Estado tem de levar a cabo para enfrentar o cometimento de crimes.

Porém, uma distinção deve ser traçada entre a atividade do Estado no que respeita àquilo que pode ser considerado como segurança pública (prevenir a ocorrência de riscos ou o cometimento de crimes que ainda não tiveram lugar) e a atividade do Estado ligada à perseguição criminal (após os crimes terem sido cometidos)[6].

2.3. A utilização de sistemas de identificação biométrica (e de tecnologias de reconhecimento facial) como uma questão jurídica primeiramente respeitante à segurança pública

I. Os sistemas de identificação biométrica (e as tecnologias de reconhecimento facial) são habitualmente vistos como ferramentas importantes para a prevenção de crimes.

O seu uso para fins policiais está assim relacionado com a atividade de segurança pública do Estado (incluindo – uma outra das aplicações de inteligência artificial que podem ser usadas pelas autoridades policiais – o chamado "policiamento preditivo" ou "previsão policial"[7])[8] e não com a atividade estatal envolvendo a perseguição de crimes[9].

---

[6] Para esta distinção e a sua importância no que respeita ao direito da proteção de dados, cfr. Orlandino Gleizer / Lucas Montenegro / Eduardo Viana, *O direito de proteção de dados no processo penal e na segurança pública*, São Paulo: Marcial Pons, 2021, pp. 22-27.

[7] Sobre o policiamento preditivo ou previsão policial, cfr., *inter alia*: Simon Egbert / Matthias Leese, *Criminal futures: predictive policing and everyday police work*, London, New York, Routledge, 2021; Henning Hofmann, *Predictive Policing – Methodologie, Systematisierung und rechtliche Würdigung der algorithmusbasierten Kriminalitätsprognose durch die Polizeibehörden*, Berlin: Duncker & Humblot, 2020; Lucia M. Sommerer, *Personenbezogenes Predictive Policing – Kriminalwissenschaftliche Untersuchung über die Automatisierung der Kriminalprognose*, Baden-Baden: Nomos, 2020; Martin Thüne, *Predictive Policing – Eine interdisziplinäre Betrachtung unter besonderer Berücksichtigung polizeirechtlicher Implikationen*, Dissertation zur Erlangung des Grads eines Doktors der Rechtswissenschaft (Dr. iur.) der Universität Erfurt, Staatswissenschaftliche Fakultät, 2020; Thomas Wischmeyer, „Predictive Policing – Nebenfolgen der Automatisierung von Prognosen im Sicherheitsrecht", in *Der Terrorist als Feind? Personalisierung im Polizei- und Völkerrecht* (Hrsg. Andreas Kulick und Michael Goldhammer), Tübingen: Mohr Siebeck, 2020, pp. 193-213; Sabine Gless, "Predictive Policing – In Defense of 'True Positives'", in Bayamlıoğlu, Emre, Baraliuc, Irina / Janssens, Liisa /

II. Naturalmente, o uso de sistemas de identificação biométrica e de tecnologias de reconhecimento facial para a atividade do Estado de perseguição de crimes também é possível.

Alguns poderão aceitar que, por exemplo, as tecnologias de reconhecimento facial sejam vistas como ferramentas de investigação úteis para a identificação de suspeitos através da comparação das suas imagens ou fotografias com as incluídas em bases de dados (em especial, as públicas).

Porém, o facto dessa possibilidade ter de ser confrontada com princípios jurídicos e garantias fundamentais do Direito Processual Penal recomenda que o tema dos sistemas de identificação biométrica e das tecnologias de reconhecimento facial seja primeiro discutido no domínio da segurança pública.

Não por acaso, as questões e os problemas colocados pelos sistemas de identificação biométrica e pelas tecnologias de reconhecimento facial são muitas vezes caracterizados

---

Hildebrandt, Mireille (eds). Being profiled: cogitas ergo sum. 10 Years of Profiling the European Citizen, Amsterdam University Press, 2018, pp. 76-83; Timo Rademacher, „Predictive Policing im deutschen Polizeirecht", *Archiv des öffentlichen Rechts*, vol. 142 (2017), 3, pp. 366-416. Suscitando dúvidas sobre a respetiva eficácia, cfr. Oskas J. Gstrein / Anno Bunnik / Andrej J. Zwitter, "Ethical, legal and social challenges of predictive policing", in *Católica Law Review*, vol. 3 n.º 3 (Nov. 2019), pp. 77-98.

[8] No ponto 24 da Resolução do Parlamento Europeu, aprovada em 6 de outubro de 2021 (disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52021IP0405&from=PT), apontam-se algumas reservas quanto ao uso do policiamento preditivo. De facto, a Resolução: "adverte que, embora o policiamento preditivo possa analisar os conjuntos de dados fornecidos para a identificação de padrões e correlações, não pode dar resposta ao problema da causalidade e não pode fazer previsões fiáveis sobre o comportamento individual, pelo que não pode constituir a única base para uma intervenção; salienta que várias cidades dos Estados Unidos puseram termo à utilização de sistemas de previsão policial após auditorias; relembra que durante a missão da Comissão LIBE aos Estados Unidos, em fevereiro de 2020, os deputados ao Parlamento foram informados pelos departamentos de polícia de Nova Iorque e de Cambridge/Massachusetts que haviam gradualmente posto fim aos seus programas de previsão policial, devido à falta de eficácia, ao impacto discriminatório e a falhas práticas, optando, antes, pelo policiamento de proximidade; relembra que o policiamento de proximidade conduziu a uma diminuição das taxas de criminalidade; opõe-se, por conseguinte, à utilização da IA pelas autoridades policiais para fazer previsões comportamentais sobre indivíduos ou grupos com base em dados históricos e comportamentos passados, pertença a grupos, localização ou quaisquer outras características semelhantes, tentando, assim, identificar pessoas suscetíveis de cometer um crime".

[9] Distinguindo entre "policiar" ("policing") e "perseguir" ("prosecuting"), embora reconhecendo que os poderes policiais se expandiram significativamente e que a linha entre segurança ("security") e aplicação coerciva da lei ("law enforcement") se esbateu, cfr. Carsten Momsen / Cäcilia Rennert, "Big Data-Based Predictive Policing and the Changing Nature of Criminal Justice – Consequences of the extended Use of Big Data, Algorithms and AI in the Area of Criminal Law Enforcement", in *KriPoZ*, 3, 2020, pp. 160-172.

como questões de segurança pública e são analisados tendo em vista legítimas preocupações de segurança (v.g., de segurança nacional).

3. As preocupações essenciais com a utilização de sistemas de identificação biométrica (e de tecnologias de reconhecimento facial) mesmo para fins de segurança pública e de aplicação coerciva da lei

I. As preocupações suscitadas quanto ao uso de sistemas de identificação biométrica e de tecnologias de reconhecimento facial são normalmente o resultado da combinação de 2 (duas) diferentes (embora interrelacionadas) ideias.

Temos, em primeiro lugar, as características específicas deste tipo de sistemas de tecnologias e, em segundo lugar, os impactos potenciais destes sistemas e tecnologias nos direitos fundamentais.

II. Uma primeira fonte de preocupação diz respeito às características técnicas e precisão dos sistemas e tecnologias[10].

Por um lado, é possível referir a difusão da tecnologia de reconhecimento facial e as dificuldades de implementação de controlo humano. Por outro lado, é possível mencionar os riscos de segurança quanto à recolha e retenção de dados de reconhecimento facial, combinados com o risco de violação e mau uso de dados de reconhecimento facial. Finalmente, é possível sublinhar o risco de erros nas tecnologias de reconhecimento facial: quer por não serem capazes de identificar um rosto que está presente numa imagem, quer por identificarem uma estrutura não facial como sendo um rosto real. Este risco de erro conduziu empresas importantes a retirarem-se do mercado das tecnologias de reconhecimento facial[11].

III. Outras fontes de preocupação relacionam-se com os direitos fundamentais[12/13].

---

[10] Gabrielle M. Haddad, "Confronting the Biased Algorithm: The Danger of Admitting Facial Recognition Technology Results in the Courtroom", in *Vanderbilt Journal of Entertainment and Technology Law*, 23, 4, 2021, pp. 891-918. Porém, fazendo menção a possíveis mecanismos para garantir a precisão das tecnologias de reconhecimento facial, cfr. Vera Lúcia Raposo, "The Use of Facial Recognition Technology by Law Enforcement in Europe: a Non-Orwellian Draft Proposal", in *European Journal on Criminal Policy and Research*, Springer online, 01 June 2022, disponível em https://link.springer.com/content/pdf/10.1007/s10610-022-09512-y.pdf.

[11] Tambiama Madiega / Hendrik Mildebrath, *Regulating facial recognition in the EU*, cit., pp. 5-6.

[12] Para uma discussão adicional, cfr., *colorandi causa*: Desara Dushi, "The use of facial recognition technology in EU law enforcement: Fundamental rights implications", Global Campus of Human

Por um lado, a ideia segundo a qual mais dados, incluindo dados pessoais, estão constantemente a ser recolhidos e analisados através de dispositivos (v.g., câmeras de vigilância ou veículos autónomos), fazendo uso de tecnologia de IA aprimorada (v.g., reconhecimento facial), o que pode levar a resultados mais invasivos para a privacidade individual e a proteção de dados. Por outro lado, alguns especialistas transmitiram a sua forte convicção de que a tecnologia de reconhecimento facial poderá ter percentagens elevadas de falsos positivos/falsos negativos e que o viés desta tecnologia pode conduzir a diferentes tipos de discriminação contra certas categorias de população (v.g., menor precisão para mulheres e pessoas não brancas[14] do que para homens brancos). Em particular, o risco de tratamento discriminatório é bastante elevado no contexto de aplicação coerciva da lei. Finalmente, têm sido identificados vários riscos relacionados com a possível utilização generalizada de tecnologias de reconhecimento facial: existe uma forte possibilidade dos sistemas de reconhecimento facial serem usados para além do fim inicialmente autorizado e controlado e, consequentemente, este facto poderá: (i) colocar em risco a possibilidade de movimentação no espaço público de forma anónima; (ii) determinar um conformismo prejudicial ao livre-arbítrio; (iii) afetar as liberdades religiosas e os direitos das crianças; (iv) interferir com a liberdade de opinião e expressão da pessoa e ter um efeito negativo no direito de reunião e de associação; (v) ter um forte impacto no comportamento social e psicológico dos cidadãos; e (vi) sublinhar questões éticas importantes[15].

Rights, 2020; Michael O'Flaherty, "Facial Recognition Technology and Fundamental Rights", in *European Data Protection Law Review*, vol. 6, 2, 2020, pp. 170-173.

[13] Preocupações adicionais, mas que não podem nesta sede ser desenvolvidas, poderão também surgir da forma como cada ordenamento jurídico proceda à configuração da tutela dos direitos de personalidade e de certos direitos constitucionalmente assegurados, nomeadamente, no que tange às tecnologias de reconhecimento facial, o direito à imagem (cfr. em Portugal o artigo 79.º do Código Civil e o artigo 26.º, n.º 1 da Constituição da República Portuguesa). Sobre o direito à imagem, em Portugal, cfr. António Menezes Cordeiro, *Código Civil Comentado*, vol. I, Coimbra: Almedina, 2020, anotação ao art. 79.º, pp. 313-320, e Diogo Costa Gonçalves, *Lições de Direitos de Personalidade*, Cascais: Principia, 2022, pp. 150-151, que insere o direito à imagem no domínio dos bens jurídicos periféricos da personalidade. Para um enquadramento geral e constitucional do registo de imagem (a partir da Alemanha e acentuando a autonomização face à reserva da intimidade da vida privada) e uma análise dos regimes vigentes em Portugal sobre a captação de imagens de pessoas e do aproveitamento das provas obtidas para processos-crime, cfr. João Gouveia de Caires, "O direito à imagem e a prova", in *Prova Penal Teórica e Prática* (coord. Paulo de Sousa Mendes e Rui Soares Pereira), Coimbra: Almedina, 2019, pp. 115-157.

[14] Com esta argumentação, cfr. https://elpais.com/tecnologia/2022-07-19/policia-predictiva-el-peligro-de-saber-donde-habra-mas-delincuencia.html.

[15] Tambiama Madiega / Hendrik Mildebrath, *Regulating facial recognition in the EU*, cit., pp. 6-9.

IV. Os receios quanto à fiabilidade e precisão e em relação às possíveis violações de direitos fundamentais não parecem reduzir-se no domínio da aplicação coerciva da lei e da justiça penal.

Na exposição de motivos da Proposta de Resolução do Parlamento Europeu, de 8 de junho de 2020[16], referia-se que os riscos potenciais associados à utilização de aplicações de inteligência artificial, incluindo tecnologias de reconhecimento facial, "seriam ainda mais graves no setor da aplicação coerciva da lei e da justiça penal, uma vez que podem afetar a presunção de inocência e os direitos fundamentais à liberdade e à segurança do indivíduo, bem como a vias de recurso efetivas e a um julgamento justo".

Do considerando M. da Resolução do Parlamento Europeu, aprovada em 6 de outubro de 2021[17], também decorre que as aplicações usadas pelas autoridades policiais, incluindo as tecnologias de reconhecimento facial, "podem ter graus de fiabilidade e precisão muito variados e um impacto na proteção dos direitos fundamentais e na dinâmica dos sistemas de justiça criminal".

4. Uma perspetiva comparada sobre o uso e a regulamentação de sistemas de identificação biométrica (e de tecnologias de reconhecimento facial) para fins de segurança pública e de aplicação coerciva da lei

A utilização de sistemas de identificação biométrica (e de tecnologias de reconhecimento facial) permite às autoridades policiais fazer uma comparação entre os dados biométricos de qualquer pessoa com o rosto de uma pessoa procurada e essa comparação tem sido considerada útil em diferentes ocasiões.

Diversos países fazem atualmente uso de sistemas de identificação biométrica, tais como tecnologias de reconhecimento facial. Podem ser encontradas diferentes abordagens quanto à admissibilidade de utilização destes sistemas e tecnologias e respetiva regulamentação. Globalmente, não é possível falar em enquadramento e em exigências regulatórias estandardizados que possam ser aplicados[18].

---

[16] Disponível em https://www.europarl.europa.eu/doceo/document/LIBE-PR-652625_PT.pdf.

[17] Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52021IP0405&from=PT.

[18] Denise Almeida / Konstantin Shmarko / Elizabeth Lomas, "The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks", in *AI and Ethics*, vol. 2, 2022, pp. 377-387.

4.1. A ausência de regulamentação nos EUA no que respeita à utilização de tecnologia de reconhecimento facial

I. Os EUA são uma das principais regiões onde a tecnologia de reconhecimento facial evoluiu rapidamente[19].

Porém, a regulamentação do uso do reconhecimento facial não se desenvolveu[20].

Os governos locais e estaduais tomaram a dianteira[21], mas alguns optaram por adotar uma abordagem restritiva.

Também não surgiu legislação a nível federal, regulamentando a utilização desta tecnologia por empresas privadas ou no contexto da aplicação coerciva da lei.

Mesmo a nível estatal e local surgiram discussões sobre o uso de tecnologias de reconhecimento facial. Algumas cidades americanas baniram a tecnologia de reconhecimento facial nos espaços públicos[22]. Porém, o Estado da Califórnia adotou uma abordagem diferente: no início de 2020 foi aprovada legislação que impôs uma moratória de três anos a qualquer tecnologia de reconhecimento facial usada em *body cams* de policiais. Além disso, o *Facial Recognition and Biometric Technology Moratorium Act* de 2020[23] foi introduzido no Senado para proibir a vigilância biométrica sem autorização legal. Essa posição foi reafirmada com o *Facial Recognition and Biometric Technology Moratorium Act* de 2021, que proíbe o governo federal usar tecnologia de reconhecimento facial salvo se legalmente autorizado, retira o apoio federal a entidades policiais estaduais e locais que façam uso da tecnologia e concede um direito privado de ação[24].

II. A falta de regulamentação federal nos EUA cria um vazio jurídico no que respeita à utilização crescente de tecnologias de reconhecimento facial pelas agências nacionais de segurança.

---

[19] Denise Almeida / Konstantin Shmarko / Elizabeth Lomas, "The ethics of facial recognition...", cit., p. 377.

[20] Patrick K. Lin, "How to Save Face & the Fourth Amendment: Developing an Algorithmic Accountability Industry for Facial Recognition Technology in Law Enforcement", in *Albany Law Journal of Science and Technology* (forthcoming).

[21] Apratim Vidyarthi, "The Public Square Has Eyes (or Cameras): Anonymous Speech Under the First and Fourth Amendments in the Age of Facial Recognition", in *Fordham Intellectual Property, Media and Entertainment Law Journal*, vol. 32, No. 3, 2022, pp. 630-688 (679).

[22] Por exemplo, Berkeley, Boston, Cambridge, Minneapolis, New Orleans, Oakland, Pittsburgh, Portland, and San Francisco – Apratim Vidyarthi, "The Public Square Has Eyes (or Cameras)", cit., p. 680.

[23] Disponível em https://www.congress.gov/bill/116th-congress/senate-bill/4084.

[24] Disponível em https://www.congress.gov/bill/117th-congress/house-bill/3907/text?r=7&s=1.

Por exemplo, o FBI usa tecnologia de reconhecimento facial para possíveis pistas de investigação e o *Department of Home Security* e a CIA também usam essa tecnologia.

Além disso, alguma literatura tem apontado que a manta de retalhos da legislação existente não é suficiente, pois dá menos ênfase à proteção de dados e à privacidade[25].

4.2. O uso indiscriminado de tecnologia de reconhecimento facial no Brasil sem regulamentação específica

I. No Brasil, as autoridades policiais têm feito uso crescente de tecnologias de reconhecimento facial com o objetivo de localizar pessoas procuradas ou criminosos foragidos.

Por exemplo, durante o Carnaval de 2019 no Rio de Janeiro, quatro pessoas com mandados de prisão pendentes[26] foram presas com a ajuda de um sistema de reconhecimento facial. No mesmo ano, um sistema de reconhecimento facial instalado num dos acessos do Carnaval de Salvador ajudou a polícia brasileira a identificar um criminoso foragido[27]. Mais recentemente, em 2020, 42 foragidos da justiça foram capturados durante o Carnaval de Salvador com a ajuda de um sistema de reconhecimento facial capaz de indicar semelhanças acima dos 90%.

II. O uso da tecnologia de reconhecimento facial foi incentivado por uma portaria do ex-ministro da Justiça e Segurança Pública Sérgio Moro.

Foi iniciado um projeto-piloto para criar um programa nacional de investigação de casos mais graves, como homicídios e crimes violentos[28].

---

[25] Denise Almeida / Konstantin Shmarko / Elizabeth Lomas, "The ethics of facial recognition...", cit., p. 377.

[26] Todavia, mencionando o caso de uma mulher erradamente detida pela Polícia Militar do Rio de Janeiro, cfr.: Mateus Vaz e Greco, "Vivendo 1984 no ano de 2020 – o reconhecimento facial e a democracia", in *Boletim IBCCrim*, 340 (March 2021), disponível em https://www.ibccrim.org.br/publicacoes/edicoes/741; Antonio Wernerck, "Reconhecimento facial falha em segundo dia, e mulher inocente é confundida com criminosa já presa", in *O Globo*, 11 de julho de 2019, disponível em https://oglobo.globo.com/rio/reconhecimento-facial-falha-em-segundo-dia-mulher-inocente-confundida-com-criminosa-ja-presa-23798913.

[27] Orlandino Gleizer / Lucas Montenegro / Eduardo Viana, *O direito de proteção de dados no processo penal e na segurança pública* cit., p. 94, nota 187.

[28] Amanda Lemos, "Reconhecimento facial cresce no Brasil; vídeo explica como isso afeta você", disponível em https://www1.folha.uol.com.br/tec/2021/08/reconhecimento-facial-cresce-no-brasil-entenda-como-isso-afeta-voce.shtml.

III. Embora o reconhecimento facial se enquadre no item da Lei Geral de Proteção de Dados Brasileira, que trata de dados pessoais sensíveis, e apesar de vários problemas relacionados com a eficiência da tecnologia, a transparência e o preconceito (especialmente para pessoas negras), a tecnologia de reconhecimento facial tem sido implementada em diferentes zonas do Brasil.

De acordo com um relatório, terão ocorrido pelo menos 22 casos de reconhecimento facial pelo governo brasileiro e os sistemas que foram utilizados tiveram as suas origens na China e em Israel[29]. Em todos os casos não havia regulamentação específica contendo critérios para a utilização do reconhecimento facial e, em vários casos, os sistemas não foram considerados transparentes e confiáveis[30].

4.3. Os avanços e recuos de regulamentação na Alemanha em relação ao uso de tecnologia de reconhecimento facial

I. A possibilidade de usar tecnologias de reconhecimento facial é menos clara na Alemanha.

Vários meios de comunicação social difundiram a ideia de que cada vez mais empresas e autoridades no mundo inteiro estariam a usar inteligência artificial para reconhecimento facial (em alemão, *künstliche Intelligenz zur Gesichtserkennung*) e, por isso, conseguiram semear a ideia no público de que o uso da tecnologia de reconhecimento para fins de segurança pública também se tornaria uma realidade na Alemanha num futuro próximo.

II. Embora vários especialistas alemães tenham apontado o facto de que tais sistemas são muitas vezes pouco confiáveis[31] e preconceituosos, foi anunciada, pelo Ministro Federal do Interior (Horst Seehofer da CSU) no início de 2020, uma proposta para o uso da tecnologia de reconhecimento facial em 135 estações de comboio e aeroportos.

O Ministro tentou introduzir a videovigilância biométrica por meio da nova Lei da Polícia Federal (em alemão, *Gesetz über die Bundespolizei* ou *Bundespolizeigesetz*)[32]. Queria que a Polícia Federal alemã (em alemão, *Bundespolizei*), que já havia examinado a tecnologia num projeto piloto realizado em 2017/2018 na estação

---

[29] Amanda Lemos, "Reconhecimento facial cresce no Brasil; vídeo explica como isso afeta você", cit.
[30] Amanda Lemos, "Reconhecimento facial cresce no Brasil; vídeo explica como isso afeta você", cit.
[31] Há quem defenda que é possível contornar tais sistemas – cfr. https://www.deutschlandfunk.de/automatische-gesichtserkennung-es-ist-moeglich-die-systeme-100.html.
[32] De 1994, cuja última alteração foi efetuada em 23 de junho de 2021.

Berlin-Südkreuz[33], pudesse comparar automaticamente as imagens escaneadas com dados biométricos[34]. No entanto, a proposta foi duramente criticada por importantes membros dos partidos políticos alemães, e foi posteriormente abandonada pelo Ministro, provavelmente por causa da pressão política[35].

III. O novo Governo Federal Alemão expressou imediatamente o seu desejo de proibir o reconhecimento facial e a vigilância em massa.

O acordo de coligação (em alemão, *Koalitionsvertrag*)[36] do novo Governo, apresentado em 24 de novembro de 2021, deixou esse desejo muito claro, através da seguinte passagem: "Rejeitamos abrangente vigilância por vídeo e o uso de gravação biométrica para fins de vigilância. O direito ao anonimato tanto no espaço público quanto na Internet é para ser garantido"[37].

IV. Tanto quanto se julga saber, o uso de tecnologias de reconhecimento facial ainda não é permitido na Alemanha[38] e não parece provável que o novo Governo

---

[33] Cfr. http://rechtundnetz.com/gesichtserkennung-in-der-oeffentlichkeit-waere-automatisierte-gesichtserkennung-im-oeffentlichen-raum-zulaessig/.

[34] Cfr. https://www.zeit.de/politik/deutschland/2020-01/bundespolizeigesetz-gesichtserkennung-verzicht-horst-seehofer?utm_referrer=https%3A%2F%2Fwww.google.com%2F.

[35] A presidente do SPD, Saskia Esken, descreveu essa mudança numa rede social como uma "excessiva interferência nas liberdades civis" – „Videoüberwachung mit Gesichtserkennung ist mein zu hoher Eingriff in die Freiheitsrechte. Die falsch positiven Fehlalarme schaden der Sicherheit mehr als die Überwachung ihr nutzt. Unschuldige Menschen geraten ins Visier" (disponível em https://twitter.com/eskensaskia/status/1213512046957989888). Antes disso, em 21.11.2018, já tinha expressado um ponto de vista idêntico: „Videoüberwachung und Datenabgleich für jedermann, um eine Ordnungswidrigkeit zu verfolgen, die nur begehen kann, wer von der Automobilindustrie betrogen und im Stich gelassen wurde? Ich halte das für unverhältnismäßig" (disponível em https://mobile.twitter.com/eskensaskia/status/1065156838008733696).

[36] Disponível em https://www.bundeskanzler.de/resource/blob/1830100/1990812/04221173eef9a6720059cc353d759a2b/2021-12-10-koav2021-data.pdf?download=1.

[37] Cfr. https://www.euractiv.de/section/innovation/news/neue-bundesregierung-will-gesichtserkennung-und-massenueberwachung-verbieten/: „„Flächendeckende Videoüberwachung und den Einsatz von biometrischer Erfassung zu Überwachungszwecken lehnen wir ab. Das Recht auf Anonymität sowohl im öffentlichen Raum als auch im Internet ist zu gewährleisten", heißt es in der Vereinbarung". Na p. 109 do acordo de coligação está escrito: "Videoüberwachung kann die Präsenz einer bürgernahen Polizei nicht ersetzen, sie aber an Kriminalitätsschwerpunkten ergänzen. Flächendeckende Videoüberwachung und den Einsatz von biometrischer Erfassung zu Überwachungszwecken lehnen wir ab. Das Recht auf Anonymität sowohl im öffentlichen Raum als auch im Internet ist zu gewährleisten".

[38] Orlandino Gleizer / Lucas Montenegro / Eduardo Viana, *O direito de proteção de dados no processo penal e na segurança pública* cit., p. 94, nota 188. Para uma discussão mais ampla sobre

Federal alemão venha a apresentar qualquer proposta no sentido de favorecer o seu uso, mesmo que para fins de segurança pública.

É verdade que uma expansão da vigilância policial por vídeo[39] ocorreu em algumas partes da Alemanha, nomeadamente em Frankfurt. No entanto, a polícia de Frankfurt não está a fazer uso do reconhecimento facial automático (que integra a chamada "videovigilância inteligente" – *intelligente Videoüberwachung* – e não se confunde com a chamada "videovigilância clássica" – *klassische Videoüberwachung*)[40], embora o chefe de polícia de Frankfurt tenha expressado a opinião de que continuará monitorando os desenvolvimentos técnicos dos sistemas de reconhecimento facial[41].

---

o tema na literatura alemã, cfr., *inter alia*: Stephan Schindler, *Biometrische Videoüberwachung – Zur Zulässigkeit biometrischer Gesichtserkennung in Verbindung mit Videoüberwachung zur Bekämpfung von Straftaten*, Baden-Baden: Nomos, 2021; Florian Kowalik, *Die hoheitliche Videoüberwachung des öffentlichen Raums zur Kriminalprävention: Rechtsgrundlagen, praktische Anwendungsbereiche und präventive Wirksamkeit*, Berlin, Münster: Lit, 2021; AA.VV., *Algorithmic policing – Chancen und regulative Herausforderungen* (Hrsg. Kristin Pfeffer), Göttingen: Cuvillier, 2022.

[39] Isto apesar das dúvidas anteriormente colocadas sobre a eficácia da videovigilância para combater o crime, uma vez que se entendia que os seus efeitos permaneciam modestos e que a videovigilância só teria sucesso se conjugada com outros esforços policiais, tal como já sublinhado em AA.VV., *Polizeiliche Videoüberwachung öffentlicher Räume* (Hrsg. Hans-Jörg Bücking), Berlin: Duncker & Humblot, 2007. Sobre essas dúvidas, com argumentos a favor e contra a utilização de videovigilância, cfr.: Dominique Maximini, *Polizeiliche Videoüberwachung öffentlicher Straßen und Plätze zur Kriminalitätsprävention*, Saarbrücken: Alma Mater, 2010, em especial pp. 14 e ss.; Gabriele Kett-Straub, „Dient die Technoprävention der Vermeidung von Kriminalität? – Insbesondere die Wirksamkeit der Videoüberwachung im öffentlichen Raum", in ZStW, vol. 123 (2011), pp. 110-133; e, mais recentemente, cfr. Martin Kutscha, „Videoüberwachung öffentlicher Plätze – ein Allheilmittel?", in *Recht und Politik*, vol. 54 (2018), 1, pp. 1-3. Criticando alguns excessos na interpretação e aplicação do direito da proteção de dados nesta matéria, cfr. Hans Peter Bull, „Fehlentwicklungen im Datenschutz am Beispiel der Videoüberwachung", in *Juristen Zeitung*, vol. 72 (2017), 17, pp. 797-806.

[40] Sobre estas distinções e outras formas de videovigilância (incluindo a videovigilância clássica, o reconhecimento automático de matrículas, a videovigilância inteligente e os drones de vídeo – *klassische Videoüberwachung*, *automatisierte Kennzeichenerfassung*, *intelligente Videoüberwachung* e *Videodrohnen*), com desenvolvimento, cfr. Elisa Stettner, *Sicherheit am Bahnhof- Überwachungsmaßnahmen zur Abwehr terroristischer Anschläge*, Berlin: Duncker & Humblot, 2017, em especial, pp. 74 e ss. Especialmente sobre a videovigilância inteligente, cfr.: Cornelius Held, *Intelligente Videoüberwachung – Verfassungsrechtliche Vorgaben für den polizeilichen Einsatz*, Berlin: Duncker & Humblot, 2014; Monika Desoi, *Intelligente Videoüberwachung – Rechtliche Bewertung und rechtsgemäße Gestaltung*, Wiesbaden: Springer, 2018.

[41] Cfr. https://www.faz.net/aktuell/rhein-main/videoueberwachung-in-frankfurt-schlechte-zeiten-fuer-kriminelle-17499671.html. Os sistemas de reconhecimento facial, tal como outros sistemas de videovigilância inteligente, apresentavam algumas dificuldades técnicas, o que permitia a alguma doutrina contrapor benefícios e receios esperados com o uso de novas tecnologias em matéria de videovigilância – assim, por exemplo, cfr. Dominique Maximini, *Polizeiliche Videoüberwachung öffentlicher Straßen und Plätze zur Kriminalitätsprävention*, cit., pp. 194 e ss.

No centro de Frankfurt, após alguma resistência inicial do Partido Político "Os Verdes" (em alemão, "*Die Grünen*"), tal expansão foi recentemente aprovada na sequência de terem ocorrido vários ataques contra pessoas LGBT[42].

4.4. As limitações decorrentes para o Reino Unido do caso *Edward Bridges v. The Chief Constable of South Wales Police*

I. A situação no Reino Unido parece mais favorável ao uso de sistemas de identificação biométrica para fins de segurança pública e de aplicação coerciva da lei.

Embora a adequação contínua do Reino Unido em termos de alinhamento com o RGPD da União Europeia continue a ser julgada pela União Europeia, mesmo após a saída do Reino Unido[43], costuma dizer-se que as forças policiais na Inglaterra usam o reconhecimento facial para combater a violência grave.

No entanto, um caso interessante sobre o uso do reconhecimento facial pela polícia surgiu no Reino Unido, mais precisamente no País de Gales, em 2019.

II. O caso é conhecido como o caso *Edward Bridges v. Chief Constable of South Wales Police* 2020.

Por vezes, diz-se que foi o primeiro caso no mundo a lidar com o reconhecimento facial automático[44]. O tribunal considerou ilegal o uso de reconhecimento facial na ausência de diretrizes claras.

III. O caso foi instaurado com base no RGPD europeu e no *Human Rights Act* de 1998.

Edward Bridges, um ativista dos direitos civis, argumentou que a ativa tecnologia de reconhecimento facial implementada pela Polícia de Gales do Sul em reuniões públicas infringiu o direito ao respeito pela vida humana de acordo com o *Human Rights Act* e os seus direitos de privacidade de acordo com o *Data Protection Act* de 2018 (DPA, de 2018), isto é, a implementação do RGPD no Reino Unido.

---

[42] Cfr. https://ddrm.de/temporaerer-ausbau-der-polizeilichen-videoueberwachung-beim-christopher-street-day-in-frankfurt/.

[43] Denise Almeida / Konstantin Shmarko / Elizabeth Lomas, "The ethics of facial recognition...", cit., p. 380.

[44] Barrie Gordon, "Automated Facial Recognition in Law Enforcement: The Queen (On Application of Edward Bridges) v The Chief Constable of South Wales Police", PER / PELJ 2021(24) – DOI, 2021, disponível em https://perjournal.co.za/article/view/8923/16871, p. 2.

Também alegou que, como a polícia não respondeu por essa infração, a avaliação do impacto na proteção de dados (*Data Protection Impact Assessment* – DPIA) também não foi realizada corretamente.

IV. O tribunal de recurso decidiu a favor de Bridges, concordando com a sua posição e, além disso, descobriu que a polícia dispunha de uma discricionariedade muito ampla em relação ao uso de tecnologias de reconhecimento facial[45].

O tribunal referiu que a aplicação coerciva da lei não está impedida de usar novas tecnologias, como o reconhecimento facial automatizado. Pelo contrário: "É de suma importância que as agências de aplicação coerciva da lei aproveitem ao máximo as técnicas disponíveis da tecnologia moderna e da ciência forense". No entanto, o agente de aplicação coerciva da lei deve permanecer dentro dos parâmetros da lei ao implementar qualquer nova tecnologia.

O tribunal de recurso reconheceu que os algoritmos de reconhecimento facial da Polícia de South Wales foram construídos em torno da proteção de dados. No entanto, isso não foi considerado suficiente pelo tribunal. As tecnologias de reconhecimento facial foram implementadas indiscriminadamente, o que violava a privacidade por definição. De facto, a quantidade de dados pessoais recolhidos foi vista como desproporcional em relação ao objetivo pretendido de identificar indivíduos em listas de vigilância (*watch lists*)[46].

Assim, o tribunal de recurso concluiu que: (i) a utilização do reconhecimento facial automatizado pela Polícia de South Wales não estava em conformidade com a lei para efeitos do artigo 8.º, n.º 2, da Convenção Europeia dos Direitos Humanos; (ii) a Avaliação de Impacto de Proteção de Dados (DPIA) da parte demandada não cumpriu com a seção 64(3)(b) da Lei de Proteção de Dados de 2018 (DPA, de 2018); (iii) e a parte demandada não se desincumbiu do seu Dever de Igualdade no Setor Público (*Public Sector Equality Duty*).

4.5. O *National Automated Facial Recognition System* vigente na Índia

I. Um uso crescente de câmeras de reconhecimento facial em espaços públicos também surge documentado na Índia.

O governo indiano colocou em vigor o *National Automated Facial Recognition System* (NAFRS), que foi desenvolvido pelo *National Crime Records Bureau* (NCRB)

[45] Denise Almeida / Konstantin Shmarko / Elizabeth Lomas, "The ethics of facial recognition...", cit., p. 382.
[46] Denise Almeida / Konstantin Shmarko / Elizabeth Lomas, "The ethics of facial recognition...", cit., p. 382.

sob os auspícios do Ministério da Administração Interna (*Ministry of Home Affairs*)[47], e aprovou a sua implementação a nível federal em 2020[48].

II. O *National Crime Records Bureau* da Índia teve como objetivo desenvolver e utilizar um banco de dados nacional de fotografias que deveria ser usado em conjunto com um sistema de tecnologia de reconhecimento facial pelas agências de segurança central e estadual.

Por esse motivo, lançou em 2019 um pedido de propostas para a criação de uma base de dados nacional de fotografias, que se destinava a ser utilizada para identificar rapidamente criminosos através da recolha de dados existentes de várias outras bases de dados, tais como: (i) Base de dados de passaportes do Ministério dos Negócios Estrangeiros (*Ministry of External Affairs*); (ii) Rede e Sistemas de Rastreamento Criminal e de Criminosos (*Crime and Criminal Tracking Network and Systems* – CCTNS) pelo *National Crime Records Bureau* (NCRB) sob o Ministério da Administração Interna; (iii) Sistema Interoperável de Justiça Criminal (*Interoperable Criminal Justice System* – ICJS) pelo NCRB sob o Ministério da Administração Interna; (iv) Portal KhoyaPaya do Ministério do Desenvolvimento da Mulher e da Criança; (v) Sistema Automatizado de Identificação de Impressões Digitais (*Automated Fingerprint Identification System* – AFIS) pelo NCRB sob o Ministério da Administração Interna; (vi) Qualquer outro banco de dados de imagens disponível com a polícia/outras entidades[49].

III. O objetivo de instituir um sistema de reconhecimento facial em todo o país resultou do teste de um software de reconhecimento facial, que foi usado pela polícia de Delhi em abril de 2018 para identificar e resgatar 3.000 crianças desaparecidas, em quatro dias[50].

O *National Automated Facial Recognition System* instituiu uma enorme rede de tecnologia de reconhecimento facial conhecida como sistema de reconhecimento facial automatizado (*automated facial recognition system* – AFRS), que torna o monitoramento de CCTV muito mais fácil ao extrair biometria facial de imagens e

---

[47] Cfr. https://internetfreedom.in/watch-the-watchmen-series-part-4-the-national-automated-facial-recognition-system/.

[48] Cfr. o comunicado de imprensa do Governo indiano de 4 de março de 2020, disponível em https://www.mha.gov.in/sites/default/files/PR_RSUSQ1495AFRS_03042020.pdf.

[49] Cfr. https://internetfreedom.in/watch-the-watchmen-series-part-4-the-national-automated-facial-recognition-system/.

[50] Cfr. https://en.wikipedia.org/wiki/Automated_Facial_Recognition_System.

combiná-las com fotografias armazenadas num banco de dados. O AFRS usa registos policiais e é acessível apenas às agências de aplicação coerciva da lei.

IV. A justificação para a implementação de um tal sistema na Índia residiu em razões de segurança nacional[51].

Os beneficiários desse sistema seriam o *National Crime Records Bureau*, as forças policiais estaduais e o Ministério da Administração Interna.

V. Apesar da justificação e da restrição do círculo de beneficiários, a literatura tem apresentado vários argumentos contra o *National Automated Facial Recognition System*.

Alguns apontaram que o sistema representa uma ameaça à privacidade[52] (protegida pelo artigo 21 da Constituição indiana) e aos direitos humanos fundamentais (como o direito à privacidade, proteção de dados, liberdade de expressão e liberdade de reunião e associação). Várias preocupações também foram manifestadas em relação ao facto de o uso do reconhecimento facial vir a permitir ao governo indiano identificar os pormenores dos manifestantes, prejudicando a liberdade individual de opinião e expressão, o direito de protesto e o direito de circulação da pessoa. Isso porque, embora os dados biométricos sejam vistos como dados pessoais sensíveis e ainda que existam procedimentos para a sua recolha, divulgação e troca, tais restrições aplicam-se apenas às "empresas" e não ao governo indiano[53].

Outros também concluem que "a implementação do NAFRS é ilegítima e não é proporcional à sua necessidade porque carece de autorização legal e diretrizes para limitar o seu uso a casos exaustivamente listados e estritamente definidos" e que, "na ausência de salvaguardas, como a lei de proteção de dados, tem o potencial

---

[51] De acordo com o comunicado de imprensa do Governo indiano de 4 de março de 2020 (disponível em https://www.mha.gov.in/sites/default/files/PR_RSUSQ1495AFRS_03042020.pdf), "This will facilitate better identification of criminals, unidentified dead bodies and missing/found children and persons. It will not violate privacy".

[52] Alguns referiram que o NAFRS não cumpre os três testes indicados pelo Supremo Tribunal no caso *Justice K.S. Puttaswamy vs Union of India* (2017) – https://blog.forumias.com/national-automated-facial-recognition-system-nafrs-explained-pointwise/. Sobre a importância do caso Puttaswamy, cfr. Cyril Amarchand Mangaldas, "Right To Privacy: Surveillance In The Post-Puttaswamy Era", December 11, 2019, disponível em https://www.bloombergquint.com/law-andpolicy/right-to-privacy-surveillance-in-the-post-puttaswamy-era.

[53] Naman Mehta / Naman Jain, "Rise in Facial Recognition Surveillance and its Implications for India in Coming Decades; Violation of Privacy and Human Right", June 30, 2021, disponível em SSRN: https://ssrn.com/abstract=3877325 ou http://dx.doi.org/10.2139/ssrn.3877325.

de vigilância em massa que afetará significativamente os direitos fundamentais e as liberdades civis"[54].

Outros até sugeriram que uma moratória sobre o uso da tecnologia de reconhecimento facial deveria ser imposta até que uma lei de proteção de dados forte e significativa fosse promulgada[55].

Uma crítica mais séria foi apresentada contra o uso de tal sistema para fins de aplicação coerciva da lei e judiciais: "A lei indiana é desprovida de qualquer legislação abrangente que autorize, regule e determine o valor probatório das tecnologias automatizadas de reconhecimento facial (AFRTs) dentro dos nossos processos de aplicação da lei doméstica e do sistema de justiça criminal mais amplo"[56].

Apesar das fortes críticas, o *National Automated Facial Recognition System* encontra-se ainda em vigor na Índia.

5. A estratégia da União Europeia para a Inteligência Artificial e para os sistemas de identificação biométrica

No contexto da União Europeia, os parâmetros críticos para o desenvolvimento e uso de sistemas de identificação biométrica e tecnologias de reconhecimento facial são fornecidos pelas regras de proteção de dados, privacidade e não discriminação, bem como pela Proposta de Regulamento sobre a Inteligência Artificial de 21 de abril de 2021.

No entanto, a abordagem da União Europeia não se restringe a esses quadros jurídicos. Vários outros requisitos da União Europeia também devem ser levados em consideração, tais como os direitos das crianças e dos idosos, a liberdade de expressão e a liberdade de reunião e associação, o direito a uma boa administração, bem como o direito a um recurso efetivo. Além disso, os sistemas de identificação biométrica suscitam questões relevantes para a segurança dos produtos, a responsabilidade do produtor e a proteção do consumidor. Por outro lado, as leis de controle das fronteiras devem ser consideradas no contexto da aplicação coerciva da lei.

---

[54] Faizan Mustafa / Utkarsh Leo, "On Facial Recognition and Fundamental Rights in India: A Law and Technology Perspective", December 29, 2021, disponível em SSRN: https://ssrn.com/abstract=3995958 or http://dx.doi.org/10.2139/ssrn.3995958.

[55] Cfr. https://www.civilsdaily.com/news/the-national-automated-facial-recognition-system-in-india-lacks-adequate-safeguards/.

[56] Cfr. Ameen Jauhar, "Facial recognition in law enforcement is the litmus test for India's commitment to "Responsible AI for All", October 17, 2021, disponível em https://www.orfonline.org/expert-speak/facial-recognition-in-law-enforcement-is-the-litmus-test-for-indias/.

5.1. A necessária articulação entre a Proposta da Comissão e outros regimes e requisitos jurídicos europeus

A Proposta de Regulamento sobre a Inteligência Artificial de 21 de abril de 2021, apresentada pela Comissão, deve ser entendida no contexto de vários outros (e anteriores) marcos e requisitos jurídicos europeus.

A este respeito, é possível dizer que existe um enquadramento multinível (*multi-level framework*) da União Europeia[57], que compreende vários enquadramentos jurídicos.

No entanto, não serão abordados nem discutidos outros enquadramentos jurídicos, já que importa concentrar a atenção na Proposta de 21 de abril de 2021.

5.2. As ideias fundamentais da Proposta da Comissão no que respeita aos sistemas de identificação biométrica

I. Os antecedentes da Proposta são o Livro Branco da Comissão Europeia sobre a Inteligência Artificial de 19 de fevereiro de 2020, bem como várias outras iniciativas do Parlamento Europeu relativas à definição de limites quanto ao uso de reconhecimento facial na União Europeia[58].

Ainda que não adote uma postura de total e permanente proibição tal como reclamada em algumas campanhas e iniciativas de cidadãos[59], a Proposta da Comissão

---

[57] Tambiama Madiega / Hendrik Mildebrath, *Regulating facial recognition in the EU*, cit., pp. 9 e ss.

[58] É o caso da Resolução do Parlamento Europeu, aprovada em 6 de outubro de 2021, iniciativa apresentada antes da Proposta da Comissão e que contém várias referências à utilização de dados biométricos e ao reconhecimento facial. Na exposição de motivos da Proposta já se reconhecia que a inteligência artificial oferece grandes oportunidades no domínio da aplicação coerciva da lei, permitindo nomeadamente melhorar os métodos de trabalho dos serviços policiais e das autoridades judiciais e combater mais eficazmente certos tipos de criminalidade, elencando um conjunto de aplicações, nas quais incluía as tecnologias de reconhecimento facial. Mas também se chamava a atenção para os riscos para os direitos fundamentais. A Resolução aprovada em 6 de outubro de 2021 reitera essas preocupações, em especial nos pontos 25, 26, 27, 30 e 31.

[59] Por exemplo, cfr. https://netzpolitik.org/2020/gesichtserkennung-kampagne-fuer-ein-dauerhaftes-europaweites-verbot/. Contra, porém, essa visão, fazendo uma apologia de 3 (três) pilares sobre os quais pode assentar um aumento da confiança pública nas tecnologias de reconhecimento facial (*stakeholder interests*, *legal and ethical considerations* e *implementation according to the varied contexts of use*) e da importância de se proceder a uma avaliação holística dos riscos e benefícios, a par de sugerir avanços no sentido da introdução de melhorias significativas nas tecnologias para reduzir imprecisões e vieses e de formação da vontade política para alcançar um consenso social sobre as salvaguardas jurídicas apropriadas, cfr. Gary K. Y. Chan, "Towards a calibrated trust-based ap-

desenvolve o tema e apresenta novas ideias para regulamentar a utilização de sistemas de identificação biométrica no contexto europeu.

A Proposta de 21 de abril de 2021 dá um passo adiante do ponto de vista da regulamentação, prevendo a sua aplicação a todos os sistemas remotos de identificação biométrica, incluindo tecnologias de reconhecimento facial[60].

II. Uma vez que a Comissão adotou uma abordagem baseada no risco (*risk-based approach*)[61], o elemento-chave da Proposta é a distinção entre sistemas de "alto risco" (ou de "risco elevado") e sistemas de "baixo risco" (ou de "risco baixo").

Tal distinção é essencial também para o uso de tecnologias de reconhecimento facial pelas autoridades policiais.

III. Em apertada síntese, a utilização de sistemas de alto risco ou é proibida pela Proposta da Comissão ou deverá cumprir requisitos apertados consagrados na Proposta, ao passo que os sistemas de baixo risco são amplamente admitidos pela Proposta e ficam sujeitos ao cumprimento de apenas alguns requisitos.

Por exemplo, é proibido[62] o uso de sistemas de reconhecimento facial em tempo real em espaços acessíveis ao público para fins de manutenção da ordem pública, salvo se aplicáveis algumas exceções limitadas. É criada uma exceção caso os Estados-Membros decidam autorizar a utilização de tais sistemas por razões importantes

---

proach to the use of facial recognition technology", in *International Journal of Law and Information Technology*, 2021, 29, pp. 305-331, disponível em https://doi.org/10.1093/ijlit/eaab011.

[60] Tambiama Madiega / Hendrik Mildebrath, *Regulating facial recognition in the EU*, cit., p. 24.

[61] Cfr. Proposta da Comissão, p. 9. Porém, para uma crítica a este tipo de abordagem da Comissão, cfr. Fanny Hidvegi / Daniel Leufer / Estelle Massé,"The EU should regulate AI on the basis of rights, not risks", 17 de fevereiro de 2021, disponível em https://www.accessnow.org/eu-regulation-ai-risk-based-approach/.

[62] Sublinha Vera Lúcia Raposo, "Ex machina: preliminary critical assessment of the European Draft Act on artificial intelligence", in *International Journal of Law and Information Technology*, 2022, 30, pp. 88-109 (94-95), que, neste particular, a Proposta da Comissão se desvia do Livro Branco, o qual se limitava a recomendar a introdução das necessárias cautelas no uso para fins de identificação biométrica remota, e igualmente vai mais longe do que a Diretiva (UE) 2016/680, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares 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 (disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L0680&from=PT), a qual também não proíbe tecnologias de reconhecimento facial e limita-se a formular exigências.

de segurança pública e desde que sejam concedidas as autorizações judiciais ou administrativas adequadas[63].

O uso de tecnologias de reconhecimento facial para fins que não sejam de manutenção da ordem pública (por exemplo, controle de fronteiras, mercados, transporte público e até escolas) é permitido, mas sujeito a uma avaliação de conformidade e cumprimento com alguns requisitos de segurança antes de poderem entrar no mercado da União Europeia[64].

Os sistemas de baixo risco estão apenas sujeitos a limitados requisitos de transparência e informação. Esse pode ser o caso de sistemas de reconhecimento facial usados para fins de categorização[65].

5.3. A aceitação limitada de sistemas de identificação biométrica para fins de segurança pública e de aplicação coerciva da lei

I. A Proposta da Comissão apresenta outra distinção relevante.

Importa distinguir entre os sistemas de identificação biométrica remota (à distância) "em tempo real" e os sistemas de identificação biométrica remota (à distância) "em diferido"[66]. Além disso, diferentes conjuntos de regras são fornecidos na Proposta, dependendo de o uso dos sistemas remotos ocorrer em tempo real ou em diferido.

II. Essa distinção surge claramente traçada na Proposta[67].

Com os sistemas de identificação biométrica remota (à distância) "em tempo real" é possível recolher dados biométricos e executar os processos de comparação e identificação instantaneamente (ou sem um atraso significativo), com base em material "ao vivo" ou "quase ao vivo", tais como imagens de vídeo, geradas por uma câmera ou outro dispositivo com funcionalidade semelhante.

Em contraste, os sistemas de identificação biométrica "em diferido" permitem a recolha de dados biométricos e executar processos de comparação e identificação, mas após um atraso significativo, com base em imagens ou imagens de vídeo geradas por câmeras de televisão em circuito fechado (CCTV) ou dispositivos privados.

---

[63] Tambiama Madiega / Hendrik Mildebrath, *Regulating facial recognition in the EU*, cit., p. 25.
[64] Tambiama Madiega / Hendrik Mildebrath, *Regulating facial recognition in the EU*, cit., pp. I e 24-25.
[65] Tambiama Madiega / Hendrik Mildebrath, *Regulating facial recognition in the EU*, cit., p. 27.
[66] Cfr. considerando 8 da Proposta da Comissão.
[67] Tambiama Madiega / Hendrik Mildebrath, *Regulating facial recognition in the EU*, cit., p. 25.

III. Para fins de manutenção da ordem pública, a Proposta proíbe a utilização de sistemas de inteligência artificial para identificação biométrica remota (à distância) "em tempo real" ou "ao vivo" de pessoas singulares em espaços acessíveis ao público[68].

Assim, não é permitido o uso pela polícia de sistemas de reconhecimento facial para identificar pessoas que participem num protesto público, ou mesmo para localizar pessoas que tenham cometido apenas pequenos delitos. Estes sistemas seriam considerados sistemas de alto risco de acordo com a Proposta da Comissão e, consequentemente, estariam sujeitos a uma proibição geral[69].

IV. No entanto, nas subalíneas da alínea *d)* do n.º 1 do artigo 5.º, a Proposta da Comissão inclui 3 (três) situações em que podem ser permitidos sistemas de identificação biométrica remota (à distância) em tempo real de alto risco para fins de manutenção da ordem pública[70].

Em primeiro lugar, a busca direcionada de potenciais vítimas específicas de crime, incluindo crianças desaparecidas. Em segundo lugar, a prevenção de uma ameaça específica, substancial e iminente à vida ou à segurança física de pessoas ou de um ataque terrorista. Em terceiro lugar, a deteção, localização, identificação ou instauração de ação penal relativamente a um infrator ou suspeito de uma infração penal referida na Decisão-Quadro do Mandado de Detenção Europeu (ou seja, um crime grave)[71].

Subjacentes a estas 3 (três) exceções estão importantes razões de segurança pública que justificam o uso de sistemas de identificação biométrica remota (à distância) em tempo real para fins de manutenção da ordem pública[72]. Não obstante, a Proposta da Comissão deixa aos Estados-Membros a decisão de aplicar as exceções. Isto porque as questões de segurança nacional continuam, em grande medida, a ser da competência exclusiva dos Estados-Membros. Em qualquer dos casos, a utilização de sistemas de identificação biométrica deve respeitar os princípios consagrados no RGPD e deve ser acompanhada de salvaguardas processuais adequadas (por exemplo, em regra, deve ser concedida uma autorização expressa e específica por uma autoridade judiciária ou por uma entidade administrativa independente)[73].

---

[68] Cfr. artigo 5.º, n.º 1, alínea *d)* da Proposta da Comissão.
[69] Tambiama Madiega / Hendrik Mildebrath, *Regulating facial recognition in the EU*, cit., p. 25.
[70] Cfr. artigo 5.º, n.º 1, alínea *d)* da Proposta da Comissão.
[71] Tambiama Madiega / Hendrik Mildebrath, *Regulating facial recognition in the EU*, cit., pp. 25-26.
[72] No entender de Vera Lúcia Raposo, "Ex machina: preliminary critical assessment of the European Draft Act on artificial intelligence", cit., p. 95, as exceções estão possivelmente justificadas por potenciais benefícios para controlar o crime.
[73] Tambiama Madiega / Hendrik Mildebrath, *Regulating facial recognition in the EU*, cit., p. 26. Cfr. artigo 5.º, n.ºs 2, 3 e 4 da Proposta da Comissão.

V. Outras possíveis utilizações de sistemas de identificação biométrica por parte das autoridades responsáveis pela aplicação coerciva da lei podem cair nas limitações da Proposta, sempre que os sistemas sejam caracterizados como sistemas de "alto risco".

Por exemplo, o uso de sistemas remotos pelas autoridades policiais para identificar uma pessoa que cometeu um crime é limitado. Além disso, o uso de sistemas de tempo real pelas autoridades policiais, mesmo em espaços não acessíveis ao público (ou seja, locais privados), também é limitado. Tais sistemas não são proibidos por si só, mas o seu uso estará sujeito ao cumprimento de vários deveres de conformidade: certos requisitos obrigatórios para garantir que o seu uso não apresenta riscos inaceitáveis; requisitos rigorosos de pré-mercado; procedimentos rigorosos de avaliação da conformidade *ex ante*; conformidade com os requisitos do RGPD; um sistema *ex post* de fiscalização do mercado e supervisão desses sistemas[74].

6. Considerações finais

I. Os sistemas de identificação biométrica, incluindo aplicativos ou tecnologias de reconhecimento facial, podem ser muito úteis para fins de verificação, identificação e categorização por parte de agentes públicos ou privados.

Muitos países estão fazendo ativamente uso de sistemas de reconhecimento facial na atualidade. Apesar das campanhas e iniciativas no sentido da sua proibição dentro e fora do espaço europeu, é improvável que pare o crescimento exponencial do uso desse tipo de sistemas no futuro, considerando a proliferação da inteligência artificial, das redes sociais, dos computadores, dos smartphones e das câmeras. O uso de tais tecnologias para fins de aplicação coerciva da lei também é geralmente reconhecido como uma realidade ou, pelo menos, considerado como uma forte possibilidade em vários países e jurisdições.

II. Ao mesmo tempo, várias preocupações têm sido suscitadas em relação ao risco de vigilância estatal ou de vigilância massiva e também no que respeita aos perigos para os direitos fundamentais.

Estas preocupações são crescentes e amplificadas pelo facto de, até à data, se detetar em vários países e jurisdições a falta de regras juridicamente vinculativas e, quando estas existem, apresentam-se na verdade muito limitadas ou até insuficientes. Falta uma legislação abrangente.

---

[74] Tambiama Madiega / Hendrik Mildebrath, *Regulating facial recognition in the EU*, cit., pp. 26-27.

III. Diversas vantagens e desvantagens têm sido identificadas relativamente ao uso de sistemas de reconhecimento facial, as quais precisam de ser enfrentadas.

Com impacto jurídico mais direto, cumpre assinalar que as principais desvantagens estão relacionadas com a difusão e o caráter intrusivo desses sistemas, bem como com a sua propensão para a ocorrência de erros. Por esse motivo, têm sido manifestadas várias preocupações com os direitos fundamentais, as quais não parecem reduzir-se (antes pelo contrário) no domínio da aplicação coerciva da lei e da justiça penal. Algumas dessas preocupações prendem-se com o facto de os sistemas de reconhecimento facial serem geradores de discriminação contra determinados segmentos da população, ao passo que outras preocupações se relacionam com a circunstância de tais sistemas poderem implicar claras violações ao direito à proteção de dados e à privacidade. Todas essas preocupações devem estar em cima da mesa, pois são relevantes para avaliar as possibilidades de uso de tecnologias de reconhecimento facial para fins de segurança pública e aplicação coerciva da lei.

IV. Tomando em consideração as vantagens e as desvantagens dos sistemas de identificação biométrica em geral e das tecnologias de reconhecimento facial, a Proposta de Regulamento sobre a Inteligência Artificial, divulgada pela Comissão em 21 de abril de 2021, incluiu novas e importantes regras sobre o tema.

Essas regras regulam a utilização de tecnologias de reconhecimento facial na União Europeia e a proposta apresentada pela Comissão propõe-se diferenciar os sistemas de identificação biométrica de acordo com as suas características de utilização de "alto risco" ou de "baixo risco". Alguns (mas não todos) os sistemas de reconhecimento facial são considerados na Proposta da Comissão como sistemas de "alto risco" e, consequentemente, a proibição do seu uso ou pelo menos a necessidade de cumprir requisitos rigorosos é proposta pela Comissão.

V. Embora seja adotada uma abordagem restritiva, a Proposta da Comissão representa um importante passo em frente para regulamentar a utilização na União Europeia de sistemas de identificação biométrica em geral e de tecnologias de reconhecimento facial também para fins de segurança pública e de aplicação coerciva da lei.

Feita a comparação com o caso de outros países e jurisdições (mesmo com aqueles que já aprovaram qualquer tipo de legislação ou regras sobre a matéria, ainda que insuficientes ou limitadas), deve concluir-se que a Proposta da Comissão procura fazer um esforço para estar alinhada com outros regimes jurídicos e requisitos

europeus (v.g., proteção de dados, regras de privacidade e não discriminação, direitos das crianças e dos idosos, liberdade de expressão e liberdade de reunião e associação, direito a uma boa administração e direito a um recurso efetivo). Se assim for, a Proposta poderá vir a ser vista como uma fonte de inspiração para outros países e jurisdições no sentido de virem a aprovar legislação abrangente que permita (ainda que de forma restritiva) o uso de tecnologias automatizadas de reconhecimento facial pelas autoridades policiais e a sua inclusão no sistema de justiça criminal.