O USO DO RECONHECIMENTO FACIAL NA SEGURANÇA PÚBLICA: PROTEÇÃO OU AMEAÇA AOS DIREITOS FUNDAMENTAIS DA POPULAÇÃO?

The Use of Facial Recognition in Public Security: Protection or Threat to Fundamental Rights?

Bruna Rey[1]

Pontifícia Universidade Católica do Rio Grande do Sul

Caroline Francescato[2]

Pontifícia Universidade Católica do Rio Grande do Sul

DOI: https://doi.org//10.62140/BRCF242380728

Sumário: 1. Introdução; 2. Reconhecimento Facial e seus Impactos nos Direitos Fundamentais; 3. Teste de Proporcionalidade: o paradoxo entre segurança pública e Direitos Humanos; 4. Perspectivas Regulatórias: o EU AI Act como Referência; 5. Conclusão.

Resumo: Este artigo explora os desafios jurídicos enfrentados diante da utilização de sistemas de reconhecimento facial na segurança pública, enfatizando os riscos de violação aos direitos fundamentais da população, tais como o direito à privacidade, à proteção de dados pessoais e à liberdade de expressão. Para tanto, analisa, inicialmente, o caso Glukhin v. Rússia, julgado pelo Tribunal Europeu de Direitos Humanos (TEDH), o qual inaugurou o debate sobre os impactos do reconhecimento facial (FRT) nos direitos humanos, bem como os critérios adotados pelo TDEH, como o teste de proporcionalidade. Após, investiga o EU AI Act como um modelo regulatório e suas diretrizes para a limitação do reconhecimento facial como um modelo a ser seguido pelo Brasil. O problema proposto é a análise da

[1] Mestranda em Direito pela Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS), com bolsa CAPES/PROEX. Graduada em Direito pela Escola de Direito da PUCRS. E-mail: bruna.rey@hotmail.com.

[2] Mestranda em Direito pela Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS), com bolsa CAPES/PROEX. Graduada em Direito pela Escola de Direito da PUCRS. E-mail: francescatocaroline@gmail.com.

compatibilidade entre o uso dessa tecnologia e a proteção das liberdades individuais, especialmente diante dos riscos de repressão política, discriminação algorítmica e restrição de direitos fundamentais. Mediante a técnica de pesquisa bibliográfica e documental e por meio de abordagem exegética e comparativa, a pesquisa conclui que a crescente implementação dessa tecnologia, seja de forma pública, seja de forma privada, exige um marco regulatório robusto capaz de mitigar riscos e garantir que seu uso seja alinhado aos princípios do Estado de Direito.
Palavras-chave: Reconhecimento facial; Vigilância em massa; Direitos humanos; Teste de proporcionalidade; Regulamentação de IA.

Abstract: This article explores the legal challenges faced by the use of facial recognition systems in public security, emphasizing the risks of violating the fundamental rights of the population, such as the right to privacy, the protection of personal data, and freedom of expression. To this end, it initially analyzes the case of Glukhin v. Russia, judged by the European Court of Human Rights (ECHR), which inaugurated the debate on the impacts of facial recognition (FRT) on human rights, as well as the criteria adopted by the TDH, such as the proportionality test. Then, it verifies the existing legislation on the subject, investigating the EU AI Act as a regulatory model and analyzing its guidelines for the limitation of facial recognition and its implications for Brazil. The proposed problem is the analysis of the compatibility between the use of this technology and the protection of individual freedoms, especially in the face of the risk of political repression, algorithmic discrimination and restriction of fundamental rights. Through the technique of bibliographic and documentary research and through an exegetical and comparative approach, the research concludes that the growing implementation of this technology, whether publicly or privately, requires a robust regulatory framework capable of mitigating risks and ensuring that its use is aligned with the principles of the Rule of Law.
Keywords: Facial Recognition; Mass surveillance; Human rights; Proportionality test; AI regulation.

1. INTRODUÇÃO

Os avanços tecnológicos observados nos últimos tempos, com a utilização cada vez mais frequente e apurada de inteligência artificial, impulsionaram o uso de tecnologias de biometria - que permitem a identificação, verificação e classificação de indivíduos – para diversas finalidades, como segurança pública, controle de fronteiras, sistemas de saúde, transações financeiras, marketing, entre outros.

No Brasil, o reconhecimento facial (FRT) também já tem sido incorporado por diversos estados, como Bahia e Goiás, os quais, desde 2013 e 2014, respectivamente, fazem uso desta tecnologia para controle da segurança pública, por meio de câmeras nas estações de metrô, aeroporto, estágio de futebol e em terminais rodoviários (Radar Tecnológico: Biometria, 2024, p. 26).

Apesar de, teoricamente, a utilização desta tecnologia trazer benefícios à sociedade, o seu rápido e desenfreado crescimento traz preocupações cruciais sobre a proteção da privacidade, a segurança dos dados e as consequências éticas de sua implementação, tendo em vista que os dados biométricos utilizados se tratam de dados sensíveis e são capazes de alcançar massas populacionais, inclusive grupos vulneráveis.

Deste modo, o presente trabalho possui a seguinte problemática: a utilização do reconhecimento facial na segurança pública representa uma ameaça aos direitos fundamentais da população? Assim, a realização desta pesquisa justifica-se para analisar a compatibilidade entre o uso desta tecnologia e a proteção das liberdades individuais, especialmente diante do risco de repressão política, discriminação algorítmica e restrição de direitos fundamentais.

Parte-se da hipótese de que essa tecnologia, quando utilizada sem restrições adequadas, compromete liberdades individuais, especialmente no contexto da segurança pública. Assim, busca-se entender como a abordagem restritiva adotada pelo EU AI Act pode contribuir e servir de parâmetro para que outros países, como o Brasil, possam lidar com a regulamentação do reconhecimento facial (FRCT) e fazer uso desta tecnologia no âmbito da segurança pública sem comprometer direitos fundamentais da população.

A pesquisa utiliza como metodologia a revisão de literatura, baseada em livros e artigos científicos. Além disso, adota uma abordagem exegética e comparativa, utilizando o teste de proporcionalidade para avaliar a

compatibilidade entre o uso governamental da tecnologia e o respeito aos direitos humanos.

2. RECONHECIMENTO FACIAL E SEUS IMPACTOS NOS DIREITOS FUNDAMENTAIS

A biometria é a ciência que permite a identificação de alguém mediante a análise de atributos fisiológicos, como, por exemplo, impressão digital, face, íris e geometria, ou também mediante a análise de comportamentais mensuráveis, como expressão facial, assinatura, modo de andar, entre outros (TEFFE, 2022, p. 149). Dentre as tecnologias de biometria, merece destaque a tecnologia de reconhecimento facial (FRT), a qual é capaz de identificar, autenticar e, inclusive, classificar indivíduos por meio da análise de características extraídas de imagens ou vídeos.

No cenário mundial, a biometria, em especial a tecnologia de reconhecimento facial, tem sido utilizada para os mais diversos propósitos, como no controle de fronteiras e aeroportos, na segurança pública, em sistemas de saúde, em transações financeiras e pagamento, no marketing e no controle de acesso de computadores, celulares, condomínios, prédios públicos, etc.

Ao mesmo tempo em que a utilização desta tecnologia traz inúmeros benefícios à sociedade - principalmente no tocante à segurança pública, por permitir uma identificação rápida e precisa dos indivíduos - traz, por outro lado, diversos desafios jurídicos diante dos riscos de violação à privacidade, aos direitos e às liberdades civis.

E é justamente neste sentido que o caso Glukhin v. Rússia, julgado pelo Tribunal Europeu de Direitos Humanos (TEDH), representa um marco no debate jurídico no que diz respeito à utilização da tecnologia de reconhecimento facial na segurança pública e à intersecção entre vigilância estatal e direitos humanos na era digital.

No caso em comento, Dmitry Glukhin realizou, em 23 de agosto de 2019, uma manifestação solo no metrô de Moscou, carregando um cartaz de papelão com a imagem de Konstantin Kotov, ativista político condenado sob acusações controversas. Após capturar imagens de Glukhin publicadas em um canal público do Telegram, a polícia russa, por meio da tecnologia de reconhecimento facial, confrontou estas imagens com gravações de câmeras instaladas em estações do metrô, o que permitiu a identificação e localização de Glukhin, culminando em sua prisão no mesmo dia.

Muito embora o governo russo jamais tenha admitido o uso de FRT no caso, Glukhin foi acusado de violar procedimentos para a realização de manifestações públicas, tendo sido condenado com base em uma lei nacional, a qual exige notificação prévia para utilização de "objetos rapidamente desmontáveis", como o cartaz de papelão.

Após esgotar os recursos internos, Glukhin recorreu ao Tribunal Europeu de Direitos Humanos (TEDH), alegando que sua prisão, fundamentada em tecnologia de vigilância, representava uma violação aos direitos garantidos pelos Artigos 8, 10 e 11 da Convenção Europeia de Direitos Humanos (CEDH), quais sejam, o respeito pela vida privada e familiar, a liberdade de expressão e a liberdade de reunião e de associação.

Ao julgar o caso, o TEDH entendeu pela violação dos artigos 8 e 10 da CEDH, sob os fundamentos de que o uso do FRT para monitorar, identificar, prender e processar Glukhin teria representado uma grave interferência no direito à vida privada, bem como que as ações das autoridades russas teriam interferido injustificadamente no direito à liberdade de expressão de Glukhin, considerando que ele exercia, de forma pacífica, sua opinião sobre uma questão de interesse público. Assim, o Tribunal concluiu que a repressão, por meio da utilização de ferramentas de vigilância, de uma manifestação pacífica teria evidenciado a desproporcionalidade da medida estatal, bem como que a utilização da FRT, sem as devidas salvaguardas contra abusos e

sem supervisão adequada, seria incompatível com os valores de uma sociedade democrática.

Para avaliar a legitimidade da interferência estatal, o Tribunal utilizou-se do teste de proporcionalidade, reconhecendo que, ao manifestar uma opinião sobre questão de evidente interesse público, Glukhin estaria exercendo seu direito à liberdade de expressão, o que restringe de forma significativa as exceções admissíveis à proteção deste direito, conforme os princípios estabelecidos pela Convenção. Assim, destacou a importância de garantir que restrições à liberdade de expressão sejam fundamentadas em critérios objetivos, devidamente equilibrados e proporcionais aos objetivos legítimos que buscam alcançar, elementos indispensáveis para assegurar uma sociedade democrática.

A decisão em questão ressaltou, também, o elevado nível de intrusão representado pela utilização de FRT ao vivo, especialmente ao processar dados sensíveis capazes de revelar opiniões políticas, razão pela qual seria indispensável uma proteção legal ainda mais rigorosa que defina, de forma clara e detalhada, as condições que justificariam o uso do FRT, sua finalidade específica, as categorias de pessoas que poderiam ser alvo e as regras para o tratamento destes dados sensíveis.

Por tais razões, o caso Glukhin v. Rússia tornou-se um marco paradigmático sobre a possibilidade de utilização de tecnologias de reconhecimento facial (FRT) para a vigilância da população e a sanção de indivíduos que exercem seus direitos fundamentais, como a liberdade de expressão e o direito à vida privada. Em outros países, como a China, também já tem ocorrido casos de vigilância massiva com o uso do FRT, o que tem gerado grande preocupação. Na província de Xinjiang, por exemplo, essa tecnologia foi empregada para monitorar e oprimir pessoas da minoria étnica Uigur, o que revela os impactos potencialmente devastadores desse tipo de prática (APC, 2021).

No Brasil, a tecnologia do FRT também já tem sido utilizada, no âmbito da segurança pública, por diversos estados, como Bahia, Goiás, Ceará, São Paulo e Rio de Janeiro. No estado da Bahia, o sistema de reconhecimento facial capturou mais de 4,3 milhões de imagens, que culminaram em 42 detenções pela polícia (Farol da Bahia, 2020), enquanto que, no estado do Ceará, onde a tecnologia é aplicada em smartphones da força policial, são capturados rostos de suspeitos quando as autoridades se aproximam (*Access Now*, 2021). De acordo com estudo realizado pela *Access Now* (*Access Now*, 2021), a grande preocupação em relação a este uso gira em torno da falta de transparência dos estados quanto aos acertos e erros destas tecnologias aplicadas à segurança pública, o que pode ensejar a violação de direitos fundamentais.

Dentre os diversos riscos da utilização desta tecnologia, destacam-se: a) efeitos discriminatórios de ordem racial, social, étnica, econômica, etc., em razão do enviesamento de normas culturais e sociais dos envolvidos no tratamento dos dados biométricos; b) constrangimento às pessoas em decorrência de falha de identificação; e c) violações a diversos direitos fundamentais, como privacidade, proteção de dados pessoais e liberdade de expressão. Por esta razão, havendo limitação a direitos fundamentais pela aplicação de determinada medida, faz-se necessária análise criteriosa baseada no teste de proporcionalidade, como será abordado no próximo tópico.

3. TESTE DE PROPORCIONALIDADE: O PARADOXO ENTRE SEGURANÇA PÚBLICA E DIREITOS HUMANOS.

Conforme defendido pela doutrina, havendo qualquer limitação a direitos fundamentais, faz-se necessária uma análise criteriosa que exige três etapas principais. Em um primeiro momento, deve-se analisar se há um propósito legítimo para a interferência ao direito, isto é, se a medida atende a um objetivo específico. Posteriormente, deve-se analisar a proporcionalidade,

ou seja, se os meios adotados são adequados para alcançar o objetivo e se não existem alternativas menos restritivas para se chegar ao mesmo fim. Por fim, visando a garantia de que a medida seja compatível com os valores de uma sociedade democrática, deve-se analisar as cláusulas de restrição geral previstas (BOGDANDY, 2011, p. 610).

Esta análise aprofundada, também conhecida como teste de três níveis, permite uma revisão substancial das razões apresentadas para justificar as interferências e restrições aos direitos fundamentais. Justamente por isso, torna-se fundamental a atribuição de parâmetros para o equilíbrio de interesses no que diz respeito à avaliação da proporcionalidade, uma vez que, é através desta técnica, que se torna possível a imposição de limites racionais às atividades estatais (ALEXY, 2002, p. 599).

Neste mesmo sentido, o professor Ingo Wolfgang Sarlet (SARLET; MARINONI; MITIDIERO, 2018, p. 235) afirma que todo e qualquer ato que restringe um direito fundamental deve passar pelo critério da proporcionalidade, o qual envolve uma análise em três etapas: (1) adequação, em que se verifica se o meio utilizado é capaz de alcançar o fim proposto; (2) necessidade, também chamada de exigibilidade ou menor sacrifício, que exige a escolha do meio que menos restringe o direito entre as opções disponíveis; e (3) proporcionalidade em sentido estrito, que se aproxima da razoabilidade e envolve a ponderação.

No contexto do uso de FRT na segurança pública - ainda que esta tecnologia possa contribuir de forma significativa no combate à criminalidade, garantindo a segurança e o bem estar da população - o cumprimento rigoroso desses critérios é essencial para equilibrar os potenciais benefícios da tecnologia para a segurança estatal com a necessidade de salvaguardar os direitos fundamentais, evitando abusos e garantindo o respeito aos princípios democráticos.

Isto porque os avanços tecnológicos e a integração de grandes volumes de dados (*big data*) viabilizaram a coleta sistemática, o registro e a

classificação de informações sobre indivíduos e instituições, o que, combinado ao uso do FRT, amplia significativamente a possibilidade de controle e monitoramento estatal, dificultando a delimitação clara de alvos e, muitas vezes, resultando em vigilância indiscriminada de toda a população (BRAYNE, 2017, p. 977-1008).

E, ainda que alguns órgãos governamentais considerem a tecnologia do FRT o método mais eficiente para gestão de risco, considerando índices de criminalidade e violência, há poucos esclarecimentos e transparência sobre o tratamento dos dados pessoais e seu compartilhamento, bem como as medidas de segurança necessárias que são adotadas pelos controladores, hipóteses legais e finalidades (FRANQUEIRA; HARTMANN; SILVA, 2021).

Assim, o teste de proporcionalidade impõe limites racionais às atividades estatais, garantindo que eventuais restrições a direitos fundamentais sejam devidamente justificadas. Neste cenário, primeiramente, caberia analisar se a medida adotada alcançaria o fim almejado, o qual, no contexto do FRT, poderia ser, por exemplo, a identificação do criminoso (adequação). Secundariamente, se a medida adotada seria realmente necessária para se alcançar o fim ou se a adoção de outras medidas menos gravosas, como o trabalho policial ou apenas a utilização de câmeras de vigilância, por exemplo, poderiam cumprir a mesma finalidade (necessidade). E, por fim, se os benefícios do uso do FRT superariam todos os potenciais danos, como, por exemplo, discriminação algorítmica e afronta à liberdade de expressão (ponderação).

Sobre as indagações à luz do princípio da proporcionalidade, no caso do FRT, a adequação parece evidente, dado o seu potencial para aumentar a eficiência na segurança pública, especialmente em contextos de alta criminalidade. No entanto, a necessidade é controversa, haja vista que alternativas menos invasivas, como o trabalho policial tradicional, ainda que possam ser menos eficazes e mais onerosas, também poderiam servir à

função. E quanto à compatibilidade com valores democráticos, a utilização do FRT se mostra crítica, considerando os riscos de discriminação, com taxas ainda mais altas de erros em grupos demográficos específicos.

Exemplos internacionais reforçam essa necessidade de cuidado. No Reino Unido, o uso policial do FRT gerou controvérsias sobre a legalidade e proporcionalidade[3], enquanto nos Estados Unidos, projetos como o Facial Recognition and Biometric Technology Moratorium Act de 2020[4] buscam limitar seu uso devido a preocupações com privacidade.

Na União Europeia, o debate sobre o EU AI Act reflete essas tensões, com propostas de proibir certas práticas, como a coleta não autorizada de dados biométricos para bases de FRT, permitindo seu uso apenas em casos específicos, como buscar pessoas desaparecidas, com autorizações judiciais. Essa abordagem incorpora o teste de proporcionalidade ao exigir que o uso seja necessário, proporcional e sujeito a salvaguardas, como limites de retenção de dados e supervisão independente, alinhando-se às etapas de adequação, necessidade e ponderação.

---

[3] O Parlamento do Reino Unido, por meio do Comitê de Justiça e Assuntos Internos, iniciou uma investigação sobre o uso de tecnologia de reconhecimento facial ao vivo pelas forças policiais na Inglaterra e no País de Gales. Representantes das forças policiais e da fornecedora de algoritmos biométricos NEC defendem que a tecnologia auxilia na captura de criminosos e localização de vítimas, minimizando invasões de privacidade. Entretanto, especialistas jurídicos questionam a legalidade e as possíveis consequências do uso indevido dessa tecnologia. Dados indicam que, em 2023, a Polícia de South Wales escaneou mais de 819.000 rostos sem erros, refletindo melhorias nos algoritmos e redução de falsos positivos. Apesar disso, debates sobre a proporcionalidade e legalidade do uso do reconhecimento facial persistem. BIOMETRIC UPDATE. UK police use of facial recognition probed by lawmakers. 12 dez. 2023. Disponível em: https://www.biometricupdate.com/202312/uk-police-use-of-facial-recognition-probed-by-lawmakers. Acesso em: 26 fev. 2025.

[4] O "Facial Recognition and Biometric Technology Moratorium Act of 2020" foi apresentado no 116º Congresso dos Estados Unidos, mas não foi votado nem aprovado durante aquela sessão legislativa. Posteriormente, o projeto foi reintroduzido em sessões subsequentes do Congresso, incluindo em março de 2023, mas até o momento não foi aprovado. PRESSLEY, Ayanna. Pressley, Jayapal, Markey & Merkley Lead Colleagues on Bill to Ban Government Use of Facial Recognition and Other Biometric Technology. 7 mar. 2023. Disponível em: https://pressley.house.gov/2023/03/07/pressley-jayapal-markey-merkley-lead-colleagues-on-bill-to-ban-government-use-of-facial-recognition-and-other-biometric-technology/?utm_source=chatgpt.com. Acesso em: 26 fev. 2025.

4. PERSPECTIVAS REGULATÓRIAS: O EU AI ACT COMO REFERÊNCIA

O EU AI Act foi proposto, em 21 de abril de 2021, pela Comissão Europeia como resposta ao rápido avanço da inteligência artificial, a qual tem transformado setores como saúde, transporte e segurança, mas também tem apresentado riscos como o viés algorítmico, violações de privacidade e falta de transparência.

A União Europeia, desde sempre comprometida com a proteção de direitos fundamentais, como estabelecido na Carta dos Direitos Fundamentais da UE, reconheceu a necessidade de um marco regulatório para categorizar sistemas de IA por níveis de risco (baixo, limitado, alto e inaceitável), promovendo inovação enquanto mitiga danos potenciais. Esse contexto foi moldado por relatórios, como o *White Paper on AI* de 2020, que destacou a urgência de regulamentação para garantir que a IA respeite valores democráticos e proteja cidadãos em um ambiente tecnológico em rápida evolução (*European Commission White Paper on AI*).

O surgimento do EU AI Act também reflete uma resposta a incidentes concretos que evidenciaram os riscos da IA desregulada. Por exemplo, estudos e relatórios, como os da Agência dos Direitos Fundamentais da UE, apontaram casos de discriminação em sistemas de IA usados em recrutamento e crédito, onde algoritmos reproduziram vieses de gênero e raciais. Além disso, a expansão do uso de IA em vigilância estatal, especialmente com tecnologias como reconhecimento facial (FRT), gerou preocupações com vigilância em massa e erosão de direitos de privacidade, intensificando o debate público.

Nesse passo, as motivações específicas para o EU AI Act incluem a necessidade de abordar tecnologias de alto risco, como o reconhecimento facial (FRT), amplamente utilizado em espaços públicos por forças de segurança e que levantou alarmes sobre vigilância em massa e violações de

direitos fundamentais. Incidentes, como o uso de FRT em Londres para identificar suspeitos sem consentimento claro, e estudos mostrando taxas mais altas de erros de identificação em grupos demográficos específicos, como pessoas de pele mais escura, destacaram o potencial de discriminação e viés algorítmico (*European Parliament Briefing AI Act*).

A falta de transparência no tratamento de dados pessoais, como coleta, armazenamento e compartilhamento, também foi um fator crítico levantado por meio de relatórios da AI Now Institute, que apontaram a ausência de *accountability* em sistemas de FRT, o que compromete a confiança pública. O EU AI Act responde a esses desafios ao classificar sistemas de IA usados em *law enforcement,* incluindo FRT como de alto risco e impondo requisitos como avaliações de conformidade, gestão de riscos e supervisão humana, conforme detalhado no Artigo 9 do proposto Act (European Commission Proposal for AI Act).

Além disso, dentre suas disposições, o Act regula o FRT em tempo real e remoto, classificando-o como uma prática de alto risco devido aos potenciais impactos na privacidade, discriminação e vigilância em massa. O Artigo 5 (1) é central para essa regulamentação, proibindo o uso de sistemas de IA para identificação remota em tempo real, exceto em casos específicos, como para autoridades policiais na prevenção, investigação, detecção ou persecução de crimes graves, incluindo a salvaguarda contra ameaças à segurança pública, desde que respeite os direitos fundamentais e estejam alinhados com a lei da UE e dos Estados-membros (European Commission Proposal for AI Act). Outra exceção, também prevista no Artigo 5, (1)(h)(i), permite o uso por autoridades públicas para a busca de pessoas desaparecidas ou para a identificação de vítimas de acidentes ou desastres, igualmente sujeitas a salvaguardas para direitos fundamentais e conformidade legal.

Dessa forma, a regulamentação estabelecida pelo EU AI Act representa um modelo robusto para países que buscam equilibrar inovação tecnológica com a proteção de direitos fundamentais. A abordagem adotada

pela União Europeia, que classifica sistemas de Inteligência Artificial (IA) em diferentes níveis de risco e impõe restrições proporcionais, demonstra a importância de um marco normativo claro e fundamentado.

Ademais, o teste de proporcionalidade incorporado no regulamento europeu também garante que restrições impostas a direitos fundamentais, como privacidade e liberdade individual, sejam justificadas e compatíveis com valores democráticos, conforme argumentado no tópico anterior. Por este motivo, o reconhecimento facial, por exemplo, é tratado como uma tecnologia de alto risco, permitindo seu uso apenas em situações específicas e com garantias adicionais de transparência e supervisão.

Esse modelo poderia servir de referência para o Brasil, onde a aplicação de FRT vem crescendo sem regulamentação específica, gerando riscos como discriminação algorítmica e vigilância excessiva (ACCESS NOW, 2021; FAROL DA BAHIA, 2020)[5]. No contexto brasileiro, a Lei Geral de Proteção de Dados (LGPD) estabelece princípios essenciais para a proteção de dados pessoais, mas ainda apresenta limitações quando aplicada a sistemas de reconhecimento facial, especialmente em segurança pública.

A ausência de diretrizes específicas sobre IA deixa espaço para abusos e violações de direitos, conforme evidenciado por relatórios do Instituto Brasileiro de Defesa do Consumidor (IDEC), que apontam falta de transparência no uso de FRT e altas taxas de erro em sistemas implementados no país (FRANQUEIRA; HARTMANN; SILVA, 2021). Exemplos de uso indiscriminado incluem a implementação de reconhecimento facial no policiamento de cidades como Rio de Janeiro, onde a tecnologia tem sido

[5] No Brasil, tramita o Projeto de Lei nº 2338/23, que tem como objetivo estabelecer normas gerais de caráter nacional para o desenvolvimento, implementação e uso responsável de sistemas de inteligência artificial (IA) no Brasil. Em seu artigo 15, prevê que "no âmbito de atividades de segurança pública, somente é permitido o uso de sistemas de identificação biométrica à distância, de forma contínua em espaços acessíveis ao público, quando houver previsão em lei federal específica e autorização judicial em conexão com a atividade de persecução penal individualizada, nos seguintes casos: I – persecução de crimes passíveis de pena máxima de reclusão superior a dois anos; II – busca de vítimas de crimes ou pessoas desaparecidas; ou III – crime em flagrante". Ainda, em seu artigo 17, inciso X, considera de alto risco os sistemas biométricos de identificação.

utilizada para monitoramento de multidões e identificação de suspeitos, sem garantias adequadas de proporcionalidade e supervisão (FAROL DA BAHIA, 2020). Essa realidade exige um arcabouço regulatório que estabeleça limites claros, supervisão humana e mecanismos de *accountability* para evitar distorções e abusos que possam comprometer a privacidade e a liberdade de expressão.

Assim, a adoção de um marco regulatório inspirado no EU AI Act poderia mitigar esses problemas ao estabelecer regras proporcionais para o uso de IA, garantindo que sua aplicação respeite os direitos fundamentais e seja pautada pela transparência e controle democrático. A regulação europeia mostra que é possível equilibrar inovação tecnológica e proteção de direitos, criando salvaguardas para impedir práticas abusivas, como o uso indiscriminado de FRT em espaços públicos.

Neste sentido, a experiência da União Europeia demonstra que regulamentar não significa inibir o desenvolvimento da inteligência artificial e da tecnologia, mas sim direcioná-las para finalidades legítimas, seguras e eticamente responsáveis. No Brasil, a implementação de normas semelhantes traria maior segurança jurídica tanto para empresas quanto para cidadãos, além de fortalecer a confiança pública na adoção dessas tecnologias. A urgência dessa regulamentação é evidente, pois a ausência de regras claras pode resultar em danos irreparáveis à democracia e aos direitos fundamentais.

5. CONCLUSÃO

A crescente implementação da tecnologia de reconhecimento facial (FRT) na segurança pública requer uma abordagem cuidadosa para equilibrar os benefícios em termos de segurança com a proteção dos direitos fundamentais da população. O caso Glukhin v. Rússia, julgado pelo Tribunal Europeu de Direitos Humanos, destacou a necessidade de aplicar o teste de proporcionalidade para avaliar a compatibilidade entre o uso governamental da FRT e o respeito aos direitos humanos.

O teste de proporcionalidade, composto por três etapas - adequação, necessidade e proporcionalidade em sentido estrito - é fundamental para determinar se a interferência no exercício de direitos fundamentais é justificável. No contexto da FRT, o propósito legítimo é a segurança pública, e a tecnologia deve ser adequada e necessária para alcançar esse objetivo, sem haver alternativas menos restritivas. Além disso, os benefícios da FRT devem superar os prejuízos aos direitos fundamentais, como privacidade e liberdade de expressão.

Neste compasso, a legislação do EU AI Act fornece uma referência valiosa, pois proíbe práticas específicas de FRT, como a coleta indiscriminada de imagens faciais, e impõe restrições ao seu uso por parte das forças de segurança, com exceções bem definidas e sob supervisão judicial (*Provisions on prohibited AI practices in EU AI Act*).

Dessa forma, para aplicar efetivamente o teste de proporcionalidade em casos de vigilância estatal usando FRT, é crucial: (1) Definir claramente o propósito legítimo do uso da FRT, limitando-se a casos de crimes sérios ou ameaças significativas à segurança pública. (2) Demonstrar que a FRT é adequada e necessária para alcançar esse propósito, não havendo outros métodos menos intrusivos que possam ser igualmente eficientes. (3) Assegurar que o uso da FRT é proporcional em sentido estrito, ou seja, que os benefícios para a sociedade superam os custos em termos de privacidade e outras liberdades individuais. (4) Estabelecer mecanismos de supervisão e transparência para monitorar o uso da FRT (*accountability*) e garantir que não haja abuso ou discriminação.

Em resumo, a utilização da FRT na segurança pública pode ser compatível com a proteção dos direitos fundamentais, contanto que seja regulamentada de forma rigorosa e que seu uso seja submetido a um escrutínio constante sob o teste de proporcionalidade. Além disso, é importante notar que, apesar das medidas regulatórias, há preocupações contínuas sobre a possibilidade de abuso ou a inadequação das salvaguardas, como destacado

por legisladores e grupos de direitos civis em debates sobre o EU AI Act (Civil rights concerns regarding EU AI Act facial recognition). Portanto, a implementação e a revisão contínua de políticas e regulamentos são essenciais para garantir que a tecnologia seja usada de maneira ética e respeitosa aos direitos humanos.

Para o contexto brasileiro, onde a FRT já é utilizada em alguns estados sem regulamentação clara, é fundamental que o legislador estabeleça normas específicas, inspiradas em exemplos internacionais como o EU AI Act, para governar o uso da FRT na segurança pública. Isso incluiria a definição de casos específicos em que a FRT poderia ser utilizada, a necessidade de autorização judicial, a implementação de medidas de transparência e a realização de avaliações de impacto sobre direitos fundamentais.

Somente com uma abordagem equilibrada e bem regulamentada, podemos aproveitar os benefícios da tecnologia de reconhecimento facial sem comprometer os direitos fundamentais da população, fazendo com que esta tecnologia deixe de apresentar uma ameaça para se tornar uma efetiva medida de proteção.

REFERÊNCIAS BIBLIOGRÁFICAS:

ACCESS NOW. Tecnologia de Vigilância na América Latina: Feita no Exterior, Implantada em Casa. 2021. Disponível em: vigilancia-latam-port.pdf. Acesso em: 13 fev. 2025.

ALEXY, Robert. Teoria dos Direitos Fundamentais. Tradução de Virgílio Afonso da Silva. 2. ed. São Paulo: Malheiros Editores, 2002.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Radar Tecnológico: Biometria e Reconhecimento Facial. Brasília: ANPD, 2024. Disponível em: radar-tecnologico-biometria-anpd.pdf. Acesso em: 20 fev. 2025.

AI NOW INSTITUTE. Report on Facial Recognition. Nova Iorque: AI Now Institute, 2019. Disponível em: https://ainowinstitute.org. Acesso em: 20 fev. 2025.

BOGDANDY, Armin von; BAST, Jürgen (Ed.). Principles of European Constitutional Law. 2. ed. Oxford/München: Hart/Beck, 2011

BRAYNE, Sarah. Big Data Surveillance: The Case of Policing. American Sociological Review, v. 82, n. 5, 2017.

COMISSÃO EUROPEIA. White Paper on Artificial Intelligence: A European approach to excellence and trust. Bruxelas: Comissão Europeia, 2020. Disponível em: https://ec.europa.eu. Acesso em: 20 fev. 2025.

FAROL DA BAHIA. Sistema de Reconhecimento Facial registra 4,3 milhões de imagens no Carnaval. 2020. Disponível em: Sistema de Reconhecimento Facial registra 4,3 milhões de imagens no Carnaval - Farol da Bahia. Acesso em: 13 fev. 2025.

FRANQUEIRA, Bruna D.; HARTMANN, Ivar A.; SILVA, Lorena A. O que os Olhos não Veem, as Câmeras Monitoram: Reconhecimento Facial para Segurança Pública e Regulação na América Latina. Revista Digital de Direito Administrativo, v. 8, n. 1, p. 171-204, 2021.

PARLAMENTO EUROPEU. European Parliament Briefing: AI Act. Bruxelas, 2021. Disponível em: https://www.europarl.europa.eu. Acesso em: 20 fev. 2025.

SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. Curso de Direito Constitucional. 13. ed. São Paulo: Saraiva, 2024.

TEFFÉ, Chiara Spadaccini de. Dados pessoais sensíveis: qualificação, tratamento e boas práticas. Indaiatuba, SP: Editora Foco, 2022.

THE ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS (APC). Facial Recognition Technology and Human Rights. Surveillance and Security in the European Union and Russia. 2021. Disponível em: https://www.giswatch.org/node/6165. Acesso em: 20 fev. 2025.

UNIÃO EUROPEIA. Parlamento Europeu e Conselho. Proposal for a Regulation of the European Parliament and of the Council laying down

harmonised rules on artificial intelligence. Bruxelas, 2021. Disponível em: https://eur-lex.europa.eu. Acesso em: 20 fev. 2025.