PONTIFÍCIA UNIVERSIDADE CATÓLICA DE SÃO PAULO
PUC-SP

Thiago Alves Duarte Faerman Soares

Reconhecimento facial em tempo real e segurança púbica: perspectivas a partir do Regulamento Europeu para construção de modelo condizente com Direitos Humanos

MESTRADO EM DIREITOS HUMANOS

São Paulo
2024

Thiago Alves Duarte Faerman Soares

Reconhecimento facial em tempo real e segurança púbica: perspectivas a partir do Regulamento Europeu para construção de modelo condizente com Direitos Humanos

MESTRADO EM DIREITOS HUMANOS

Dissertação apresentada à Banca Examinadora da Pontifícia Universidade Católica de São Paulo, como exigência parcial para obtenção do título de MESTRE em Direitos Humanos, sob a orientação do Prof. Dr. Motauri Ciocchetti de Souza.

São Paulo

2024

Thiago Alves Duarte Faerman Soares

Reconhecimento facial em tempo real e segurança púbica: perspectivas a partir do Regulamento Europeu para construção de modelo condizente com Direitos Humanos

Dissertação apresentada à Banca Examinadora da Pontifícia Universidade Católica de São Paulo, como exigência parcial para obtenção do título de MESTRE em Direitos Humanos, sob a orientação do Prof. Dr. Motauri Ciocchetti de Souza.

BANCA EXAMINADORA

_____

_____

_____

_____

_____

AGRADECIMENTOS

Agradeço, primeiramente, à minha esposa e inspiração Laura Duro, companheira para todos os momentos e grande incentivadora nas horas mais difíceis. Sem o apoio dela, essa empreitada não seria possível. Agradeço, também, à minha família sanguínea, especialmente minha mãe, Maria Tereza, minha irmã Juliana e meu sobrinho Pedro, bem como à minha família por extensão, Rosana, Carlos Eduardo e Gabriel, todos essenciais para qualquer conquista que possa obter.

Gostaria, ainda, de expressar minha profunda gratidão ao Professor Doutor Motauri Ciocchetti de Souza, que me guiou nessa jornada, cujos desafios foram ímpares, mas sempre enfrentados de frente. O Doutor Motauri sempre foi referência profissional e acadêmica, de modo que detenho enorme orgulho de ter tido a oportunidade de tê-lo como orientador. Como por vezes saliento, o Doutor Motauri, também Corregedor do Ministério Público de São Paulo, instituição a qual tenho o orgulho de integrar, é meu duplo orientador, tanto do ponto de vista acadêmico, quanto do ponto de vista profissional. Espero ter feito jus à confiança em mim depositada.

Não posso deixar de agradecer, igualmente, aos Professores Doutores Alexandre Rocha Almeida de Moraes e Pedro Henrique Demercian, coordenadores do grupo de pesquisa de jurimetria da PUCSP, que, de braços abertos, me acolheram e me mostraram perspectiva de direito na seara criminal mais pragmático e atento aos efeitos concretos das posturas adotadas pelos operadores jurídicos, com a devida criticidade na abordagem de temas complexos. Especialmente ao Professor Alexandre, gostaria de enfatizar que ele foi o grande incentivador para meu ingresso no curso de mestrado, quando nem mesmo eu acreditava ser possível, pelo que guardo enorme gratidão. Agradeço, também, aos examinadores externos, Professores Doutores Fábio Ramazzini Bechara e Fausto Junqueira de Paula pela disponibilidade e dedicação na leitura de meu trabalho.

Estendo meus cumprimentos, por fim, a todos os Professores que tive nessa jornada do Mestrado, todos brilhantes, que, de alguma forma, contribuíram para o resultado desta obra. São eles os Professores Doutores: Wagner Balera, Celso Campilongo, Eduardo Dias Ferreira, Marcelo Sodré e Maria Celeste Cordeiro Leite dos Santos. Em especial, a Professora Maria Celeste foi, em grande medida, influenciadora desta dissertação, pois possibilitou análise aprofundada do Regulamento Europeu em sua cadeira, que, certamente, mudou meu percurso acadêmico.

Dedico este trabalho à memória de meu pai.

RESUMO

O presente trabalho dedicou-se a avaliar a compatibilidade das previsões de uso de reconhecimento facial na segurança pública pelo Regulamento Europeu da Inteligência Artificial com a proteção de Direitos Humanos e sua eventual compatibilidade com o ordenamento jurídico brasileiro, de modo a servir como fonte de inspiração legislativa. Partindo da ótica que a atividade de segurança pública revolve direitos fundamentais e humanos multigeracionais, dos quais decorre obrigação de agir estatal, buscou-se averiguar como a tecnologia de reconhecimento facial, impulsionada pela inteligência artificial, poderia auxiliar em tal mister. Apontou-se que o reconhecimento facial engloba gênero de diversas tecnologias direcionadas a usos e finalidades distintas. O presente trabalho, a seu turno, focou na identificação biométrica à distância em tempo real, consistente na identificação instantânea de indivíduo em meio à multidão. Adentrou-se nos aspectos técnicos e jurídicos controvertidos de referida tecnologia, que segue os passos do ciclo de vida da inteligência artificial. Estabelecida a premissa, a partir do arcabouço teórico estudado, de que referida tecnologia é passível de regulamentação para usos restritos, abordou-se o Regulamento Europeu da Inteligência Artificial, primeiramente contextualizando o diploma e após adentrando nas previsões específicas sobre o objeto de estudo. A relevância do Regulamento Europeu decorre da profundidade do diploma normativo, da tradição pátria em referendar o pensamento jurídico europeu e do chamado efeito Bruxelas. Acerca da identificação biométrica à distância em tempo real, o mencionado Regulamento vedou, em regra, seu uso para segurança pública, salvo em hipóteses excepcionais, dependentes, ainda, da observância de rígidas balizas e procedimento rigoroso perante autoridade judiciária ou equiparada para deferimento. Reputou-se que o Regulamento, apesar de eventuais pontos de melhoria, se mostra, em linhas gerais, atento aos direitos humanos e fundamentais em voga, sem prejuízo de potenciais aperfeiçoamentos ao longo de sua implementação. No Brasil, por sua vez, embora já haja uso da tecnologia, carece-se de regulamentação. Em vista às propostas europeias, concluiu-se que, embora o Regulamento se trate de relevante fonte normativa, a sua previsão genérica em determinados pontos, sem abordar questões específicas da identificação biométrica à distância em tempo real e de seus riscos particulares, acabou por deixar brechas na implementação do sistema passível de gerar violações a direitos fundamentais. Assim, em complemento às previsões do Regulamento Europeu, foram propostas sugestões para fortalecimento da regulamentação no cenário nacional em prol da proteção dos direitos fundamentais e humanos envolvidos.

PALAVRAS-CHAVE: Direitos Humanos, Identificação Biométrica à Distância em Tempo Real, Inteligência Artificial, Reconhecimento Facial, Regulamento Europeu da Inteligência Artificial, Segurança Pública.

ABSTRACT

The present work aimed to evaluate the compatibility of the European Artificial Intelligence Act regarding the use of facial recognition technology for public security purposes with the protection of Human Rights and its eventual compatibility with the Brazilian legal system, in order to serve as a source of legislative inspiration. Based on the perspective that public security activities represent multigenerational fundamental and human rights, from which the obligation of state action arises, it was sought to determine how facial recognition technology, driven by artificial intelligence, could assist in such a task. It was pointed out that facial recognition encompasses several technologies aimed at different uses and purposes. The present work focused on remote biometric identification in real-time, which consists in the instantaneous identification of an individual in a crowd. The controversial technical and legal aspects of this technology, which follows the life cycle steps of artificial intelligence, were dissected. Having established the premise, based on the theoretical framework, that it is possible to regulate such technology for restricted uses, the European Artificial Intelligence Act was approached, first contextualizing the diploma and then going into specific rules about the object of study. The relevance of the European Artificial Intelligence Act arises from the depth of the normative diploma, the brazilian tradition in endorsing European legal thought and the so-called Brussels effect. Regarding remote biometric identification in real time, the aforementioned Regulation prohibited its use for public security as a general rule, except in exceptional cases, which also depend on compliance with strict guidelines and strict procedures before a judicial or similar authority for approval. It was considered that the Regulation, despite possible points of improvement, appears, in general, to be attentive to human and fundamental rights, without prejudice to potential betterments throughout its implementation. In Brazil, although the technology is already being used, there is a lack of regulation. In view of the European proposals, it was concluded that, although the Regulation is a relevant normative source, its generic provision at certain points, without addressing specific issues of real-time remote biometric identification and its particular risks, ended up leaving loopholes in the implementation of the system that could lead to violations of fundamental rights. Thus, in addition to the provisions of the European Regulation, suggestions were proposed to strengthen regulation in the brazilian national scenario in favor of protecting the fundamental and human rights involved.

KEY-WORDS: Artificial Intelligence, European Artificial Intelligence Act, Facial Recognition, Human Rights, Public Security, Real-Time Remote Biometric Identification.

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1. INTRODUÇÃO

Embora estudos iniciais sobre o tema remontem à década de 50, é somente com o avanço tecnológico nos últimos anos, ao aumentar a capacidade de processamento das máquinas, que a inteligência artificial se torna pauta central no debate acadêmico.

Isso porque, ao mesmo tempo em que apresenta potencial de inovação sem precedentes a gerar benefícios em diversas searas da vida humana, a inteligência artificial, por se tratar de instrumental baseado em máquinas dependentes de dados (ou seja, passíveis de vieses decorrentes dos dados fornecidos) e que operam com autonomia, complexidade e opacidade, ostenta riscos em sua essência.

Nesse contexto, surgem questões sobre a medida em que tais sistemas devem ser utilizados na vida humana, de modo a extrair o melhor benefício deles, sem, por outro lado, criar riscos inaceitáveis aos indivíduos e à sociedade.

Essas questões revelam especial importância na área de segurança pública, destinada a tutelar os bens jurídicos mais valiosos do ordenamento.

A segurança pública representa direito fundamental e humano multigeracional, revolvendo a atividade estatal direcionada à prevenção e à repressão de delitos, em que emergem obrigações processuais penais positivas ao Estado na tutela da vítima e da coletividade, a serem exercidas dentro das balizas do ordenamento jurídico, de modo a não representar arbitrariedades contra os investigados.

A segurança pública contém, em seu bojo, a um só tempo, a necessidade de tutelar as vítimas e a garantir que isso ocorra sem abusos estatais na condução do processo legal, no intuito de não ferir outros direitos preconizados no ordenamento, de modo a demandar um fino ajustamento nas balizas para desempenho de tal mister pelo Estado.

Exatamente por isso é que o tema da inteligência artificial desperta tamanho interesse nas questões afetas à segurança pública, na medida em que a tecnologia, apesar de representar potenciais benefícios na consecução de mencionada atividade estatal, carrega consigo riscos que, se não bem administrados, podem resultar em violações a garantias individuais e eventualmente acentuar discriminações latentes no sistema de justiça criminal.

Dentre os usos, um dos mais polêmicos se refere ao reconhecimento facial em tempo real por câmeras presentes na via pública, capazes de identificar fugitivos, suspeitos ou vítimas por meio de inteligência artificial.

Enquanto, de um lado, existe a expectativa de que tal mecanismo melhore a eficiência da persecução criminal, sobretudo diante da constante evolução tecnológica, há notícias de falhas no sistema, resultando em abordagens errôneas e em vieses contra determinados grupos demográficos, notadamente mulheres e negros, com o potencial de incrementar padrões discriminatórios.

Diante disso, emergem questões sobre o uso de tal tecnologia para fins de segurança pública, ensejando intensos debates tanto em nível acadêmico, quanto em nível político.

Embora determinados locais, como o Município de São Francisco nos Estados Unidos, tenham banido a possibilidade de mencionado uso, a União Europeia, recentemente, em 13 de junho de 2024, publicou o Regulamento (UE) 2024/1689, destinado a regulamentar o uso da inteligência artificial, que contém disposições específicas sobre o reconhecimento facial remoto em tempo real.

Apesar de, em regra geral, o uso da tecnologia ser proibido para fins de segurança pública, referido Regulamento permite o reconhecimento facial remoto em tempo real em determinados casos, cumpridas estritas balizas fixadas no diploma normativo.

Essa regulamentação chama a atenção por se tratar de um dos primeiros diplomas normativos a tratar de forma mais aprofundada do reconhecimento facial remoto em tempo real, regulando as possibilidades de uso da tecnologia.

O interesse se revela ainda maior em solo brasileiro, em que a tecnologia é utilizada e questionada, mas se carece de qualquer diploma normativo sobre o tema. Aliás, a relevância do Regulamento se torna evidente ao se considerar tanto a tradição nacional em endossar o pensamento europeu em matéria penal e processual penal, quanto o chamado “Efeito Bruxelas”, consistente na reprodução das normativas europeias por outros países, exatamente pela influência de referidas regulações nos mercados globalizados.

Portanto, desponta a pertinência de se estudar o Regulamento quanto ao uso do reconhecimento facial remoto em tempo real.

O presente trabalho, então, tem como objetivo avaliar a compatibilidade das previsões de uso de reconhecimento facial na segurança pública pelo Regulamento Europeu da Inteligência Artificial com a proteção de Direitos Humanos e sua eventual compatibilidade com o ordenamento jurídico brasileiro, de modo a servir como fonte de inspiração legislativa.

Para tal finalidade, foram fixados os seguintes objetivos específicos: a) conceituar a segurança pública e sua relação com direitos fundamentais e humanos; b) analisar o uso de inteligência artificial e notadamente do reconhecimento facial na área de segurança pública, com cotejamento entre os potenciais benefícios e os riscos decorrentes; c) estudar o

equacionamento proposto pelo Regulamento Europeu para utilização do reconhecimento facial para fins de segurança pública; d) ponderar o uso do reconhecimento facial permitido pelo Regulamento Europeu para fins de segurança pública com os Direitos Humanos envolvidos; e) averiguar a situação do uso do reconhecimento facial para fins de segurança pública no Brasil; f) estudar a compatibilidade das previsões do Regulamento Europeu sobre reconhecimento facial com o ordenamento brasileiro e com a tutela dos Direitos Humanos.

Na busca de tais objetivos, o trabalho foi dividido em quatro capítulos, mais a presente introdução e a conclusão.

No capítulo segundo, logo após esta introdução, aborda-se o direito fundamental e humano à segurança pública, com seus respectivos desdobramentos no que diz respeito às obrigações processuais penais positivas do Estado.

No terceiro capítulo, conceituam-se as tecnologias de reconhecimento facial, delimitando-se o objeto de estudo, que se trata da identificação biométrica à distância em tempo real para fins de segurança pública, com apresentação da complexidade do tema.

Em referido capítulo, ainda, adentra-se tanto nas diversas questões jurídicas que emergem do tema, quanto nas questões técnicas relevantes que influenciam o debate jurídico. Ao final de tal capítulo, após minucioso estudo sobre a tecnologia, apresentam-se alternativas para a temática, concluindo-se que a estrita regulamentação (e não o banimento peremptório) é a melhor forma de ponderar os diversos interesses em jogo.

No quarto capítulo, analisa-se o Regulamento Europeu da Inteligência Artificial, com introdução ao tema mediante análise de aspectos gerais importantes para compreensão do diploma.

Em seguida, esmiúça-se como o Regulamento Europeu abordou a identificação biométrica à distância em tempo real, estudando-se as hipóteses excepcionais de uso de tal tecnologia, com avaliação sobre a compatibilidade da regulamentação com os direitos humanos envolvidos.

No quinto capítulo, volta-se a atenção ao território brasileiro com destaque para influência do Regulamento Europeu em solo nacional ante a carência normativa específica. Investiga-se se a proposta europeia confere solução adequada ao ordenamento pátrio para tutela de direitos fundamentais e humanos.

Ao final, apresenta-se a conclusão dos estudos, com abordagem dos conceitos relevantes vistos ao longo do trabalho, bem como dos pontos para futuras discussões.

2. SEGURANÇA PÚBLICA

A primeira tarefa do presente trabalho se destina a conceituar a segurança pública e sua relação com os direitos fundamentais e humanos.

Isso é importante, na medida em que a finalidade de uso da inteligência artificial é fundamental para definição do seu grau de risco, como será abordado nos capítulos referentes ao Regulamento Europeu.

2.1. CONCEITO

Conforme artigo 144 da Constituição Federal (Brasil, 1988, título V, cap. III, artigo 144), a segurança pública "é exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio".

O conceito de segurança pública se relaciona, portanto, com a manutenção da ordem pública, cuja definição (de ordem pública) carrega consigo, todavia, multiplicidades interpretativas (Erthal, 2020).

Segundo Moreira Neto (1991), o conceito de ordem se relaciona a uma ideia estática, pressuposto de organização, ao passo que a segurança é uma ideia dinâmica, refletindo uma atividade cuja função é a garantia dessa ordem. Em suma: "a segurança existe para evitar o comprometimento da ordem" (Moreira Neto, 1991, p. 13).

A fim de delimitar com precisão a correlação entre segurança e ordem públicas, Lazzarini (1989) acentua que a segurança pública engloba apenas parte da ordem pública, cuidando-se de conceito mais restrito, direcionado ao combate às práticas delitivas. Com efeito, ordem pública reflete conceito mais amplo, por abranger atividades como, por exemplo, medidas sanitárias e urbanas, de modo que a parcela de ordem pública protegida pela segurança pública se relaciona àquela afetada quando da ocorrência delitiva (Erthal, 2020).

Segurança pública revolve, portanto, atividades estatais de prevenção, vigilância e repressão de delitos, de modo a permitir o desenvolvimento individual (Souza Neto, 2013).

Disso, extraem-se dois pontos: primeiro, a segurança pública é uma atividade estatal, e, segundo, objetiva tutelar a ordem pública por meio da prevenção e repressão de delitos, consagrando o direito à autopreservação humana (Buonamici, 2011).

Consequentemente, a necessidade de tutela da segurança pública, entendida, então, como a atividade estatal direcionada contra a prática delitiva, se cuida de pressuposto para a construção do próprio Estado moderno, em que o Poder Público detém o monopólio do uso legítimo da força, bem como se trata, em essência, de pré-requisito para o exercício dos demais direitos fundamentais, pois, sem a atuação estatal para proteger o indivíduo, qualquer liberdade fundamental ficaria prejudicada (Ávila, 2014).

2.2. DIREITO FUNDAMENTAL

Apesar de certa imprecisão semântica na utilização do termo, prevalece que a expressão "direitos fundamentais" se refere a normas jurídicas exigíveis no âmbito interno do Estado decorrente de sua incorporação no texto constitucional (Fernandes, 2018).

Conforme Mendes e Branco (2013, p. 167): "a locução direitos fundamentais é reservada aos direitos relacionados com posições básicas das pessoas, inscritos em diplomas normativos de cada Estado", de modo que eles são assegurados "na medida em que cada Estado os consagra".

No caso brasileiro, a Constituição Federal de 1988, ao ser a primeira, na história do país, a utilizar a expressão genérica "direitos e garantias fundamentais", alinhou-se ao constitucionalismo alemão, português e espanhol, de modo a trazer, para o texto constitucional positivo, o tema dos direitos fundamentais, o que seria o local adequado para tratamento da matéria, dada a hierarquia normativa superior que tais direitos devem assumir no ordenamento jurídico interno (Sarlet, 2013).

Trata-se, então, de direitos previstos no texto constitucional com hierarquia normativa superior, dotados de regime jurídico privilegiado decorrente dessa supremacia normativa e da limitação que impõem ao poder político (Sarlet, 2013). Esse regime jurídico privilegiado, aliás, pode ser percebido, no caso brasileiro, ante a proibição de o poder constituinte derivado propor emendas constitucionais tendentes a abolir "direitos e garantias individuais", conforme artigo

60, §4º, IV, da Constituição Federal (Brasil, 1988), consagrando-os, portanto, como cláusulas pétreas.

Consequentemente, dependentes de previsão constitucional, os direitos fundamentais são dotados de historicidade, já que eles não são dados, mas a sua consagração decorre de um aspecto histórico-evolutivo (Mendes e Branco, 2013).

Seguindo nessa acepção do processo histórico-evolutivo da consagração dos direitos fundamentais, a doutrina majoritária elenca, para fins didáticos quanto ao momento de surgimento, três gerações (ou dimensões) de direitos fundamentais (que não se sobrepõem, mas se complementam).

Essa classificação é atribuída à palestra de Karel Vasak na Universidade de Estrasburgo em 1979, em que ele separou os direitos fundamentais de acordo com os temas da revolução francesa, a saber, liberdade, igualdade e fraternidade (Oliveira, 2018).

A primeira geração de direitos fundamentais, portanto, se refere a direitos de liberdade, comumente associada com direitos civis e políticos, cujo titular é o indivíduo, em que se espera do Estado uma postura negativa, isto é, a não interferência na esfera privada (Fernandes, 2018).

Ante as agruras oriundas do Estado absenteísta, sobrevém preocupação com a desigualdade social, despontando a busca por uma igualdade material e liberdade real (e não meramente formal) dos indivíduos (Mendes e Branco, 2013), de forma que advém a segunda geração de direitos fundamentais, consistentes em direitos sociais, culturais e econômicos, chamados de forma ampla de direitos sociais não por uma perspectiva propriamente coletiva, mas pela "busca da realização de prestações sociais" (Fernandes, 2018, p. 327).

A terceira geração de direitos fundamentais, por sua vez, decorre de uma noção expandida de humanidade, em que os titulares dos direitos não podem ser mais individualizados, na perspectiva de tutelar o gênero humano como um todo, o que se coaduna com o princípio da fraternidade (Fernandes, 2018).

Embora existam doutrinadores que conceituem outras gerações (Fernandes, 2018; Oliveira, 2018), o tema é controverso, prevalecendo, em boa parte da doutrina, que as mencionadas novas gerações refletem direitos que podem ser enquadrados em gerações antigas, sem necessidade de novas classificações (Mendes e Branco, 2013).

Sobre a segurança pública, é interessante observar que a própria construção do Estado ocorre para que referido ente sirva como garantidor de direitos, atuando no caso de violações. Nesse sentido, veja-se o exposto por Henry Shue (citado por Ávila, 2014, p. 162):

> Ninguém pode usufruir plenamente nenhum direito que é supostamente protegido pela sociedade se alguém puder livremente ameaçar tal pessoa de assassinato, estupro, agressões etc., quando a pessoa tentar usufruir os direitos em discussão. Tais ameaças à segurança física estão entre as mais sérias e – na maioria do mundo – os obstáculos mais difundidos ao gozo de qualquer direito. [...] Na ausência de segurança física as pessoas não são capazes de fruir qualquer outro direito que a sociedade diga estar protegendo, pois estão susceptíveis de enfrentarem muitos dos piores perigos que eles enfrentariam se a sociedade não protegesse os seus direitos.

Ou, nas palavras de Buonamici (2011, p. 07):

> O direito à segurança pública sempre esteve ligado à história da própria humanidade, presente em qualquer espécie de agrupamento humano, formal ou não, conquanto seus integrantes sempre tiveram a necessidade de proteção social, exercida pela atuação policial, para garantir a paz e a harmonia na convivência social, mormente indicados os valores principais de auto preservação da espécie humana, o direito à vida; o direito à liberdade e o direito à propriedade.

Assim, a própria existência do Estado decorre, ainda que em parte, para garantia da segurança pública das pessoas em seu território, de modo que o Estado é o detentor do monopólio do uso legítimo da força, a evitar, em decorrência, o recurso à vingança privada.

Consequentemente, antes mesmo de embasamentos jurídicos quanto à fundamentalidade da segurança pública, existem fundamentos sociológicos para a questão, que perpassam pela própria construção do Estado moderno e contemporâneo, a partir de teorias sociológicas, como, por exemplo, a de Hobbes (Ávila, 2016).

Por esse prisma, a segurança pública "se trata de um pré-requisito essencial para o exercício dos demais direitos fundamentais assegurados constitucionalmente" (Ávila, 2016, p. 162).

Relativamente ao status jurídico da segurança pública, embora em outros países exista controvérsia acerca do enquadramento do instituto como um direito fundamental ou como um

dever de proteção estatal decorrente da dimensão objetiva de outros direitos fundamentais, no Brasil não haveria espaço para tal discussão, porquanto a positivação da segurança ocorre no texto constitucional, especialmente nos artigos 5º, 6º e 144 da Carta Magna (Ávila, 2016), *in verbis* (Brasil, 1988, título II, cap. I, artigo 5º; título II, cap. II, artigo 6º; título V, cap. III, artigo 144, grifo nosso):

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à **segurança** e à propriedade, nos termos seguintes:
>
> [...]
>
> Art. 6º São direitos sociais a educação, a saúde, a alimentação, o trabalho, a moradia, o transporte, o lazer, a **segurança**, a previdência social, a proteção à maternidade e à infância, a assistência aos desamparados, na forma desta Constituição.
>
> [...]
>
> Art. 144. **A segurança pública**, dever do Estado, **direito e responsabilidade de todos**, é exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio, através dos seguintes órgãos:

Em realidade, o direito à segurança apresenta dupla fundamentalidade, tanto do ponto de vista formal quanto do ponto de vista material, nesse último aspecto como corolário da dignidade da pessoa humana, em que se necessita de previsibilidade e tranquilidade para desenvolvimento do indivíduo (Souza Neto, 2013).

Aliás, a dignidade da pessoa humana impõe feixe de deveres e direitos correlatos, indispensáveis para desenvolvimento do indivíduo, de modo a implicar uma obrigação geral de respeito ao próximo (Fischer e Pereira, 2023).

Não se perca de vista, por esse prisma, que o crime se revela como elemento violador de direitos humanos e fundamentais, cuja eficácia também incide em relações privadas (Oliveira, 2022). Não por acaso, então, há mandados constitucionais de criminalização, decorrentes dos direitos fundamentais correlatos e da própria dignidade da pessoa humana (Oliveira, 2022).

Evidente, portanto, que, se a segurança pública significa o combate ao crime, que, por sua vez, é violador de direitos fundamentais, o direito a ela, segurança pública, ainda que não

estivesse expresso no texto constitucional, decorreria dos princípios implícitos, nos termos do artigo 5º, §2, da Constituição Federal (Brasil, 1988), e como corolário da própria dignidade da pessoa humana.

Essa questão é patente, inclusive, pela própria leitura do preâmbulo da Constituição, vetor interpretativo do texto, em que se consigna, expressamente, a instituição de um "Estado Democrático, destinado a assegurar o exercício dos direitos sociais e individuais, a liberdade, a segurança [...]" (Brasil, 1988, preâmbulo).

Conceitua-se, então, o direito fundamental à segurança como a "possibilidade de exigir proteção em determinadas situações que colocam em risco evidente os bens apontados como mais valiosos" (Erthal, 2020, p. 25).

Referido direito, de índole autônoma, cuida-se, inclusive, do fundamento normativo interno das obrigações processuais penais positivas, reconhecidas pela doutrina especializada (Oliveira, 2022; Fischer e Pereira, 2023).

Deveras, como corolário dessas questões, exsurge-se o direito fundamental à efetividade do processo penal e o embasamento constitucional para as obrigações processuais penais positivas, uma vez que o Estado não pode se quedar inerte ante a violação de bens jurídicos em seu território (Oliveira, 2022). Do contrário, o Estado, ao cabo, seria tolerante a violações de direitos em seu território, desconsiderando a dignidade humana da vítima, cujos direitos foram violados (Oliveira, 2022).

Logo, a segurança pública se reflete em direito autônomo, no sentido da adoção de medidas pelo Estado para evitar violação de direitos fundamentais, não se cuidando, portanto, de mero corolário de outros direitos fundamentais. Sobre o tema, bem expôs Ávila (2016, p. 168), nos seguintes termos:

> Não se pode confundir o direito fundamental de defesa com o direito fundamental individual à segurança: enquanto o direito fundamental em si exige que outro particular se abstenha de violá-lo, o direito fundamental à segurança exige que o Estado tome as medidas necessárias para evitar a violação de um direito fundamental ou para restabelecer sua normal fruição.
>
> No exemplo dado, o direito fundamental à liberdade estabelece uma posição jurídica do cidadão contra o sequestrador (a obrigação de o sequestrador fazer cessar a restrição ilícita do direito de liberdade), enquanto o direito à segurança estabelece uma posição jurídica do cidadão contra o Estado (a obrigação de o Estado intervir para obrigar o sequestrador a fazer cessar a restrição ilícita do direito de liberdade, mediante a libertação do refém). O

> direito à segurança é instrumental em relação ao direito à liberdade e, apesar do titular do direito ser o mesmo (o refém) o sujeito passivo da relação jurídica é distinto (sequestrador e Estado). A segurança é, portanto, uma garantia jusfundamental.

Conforme Buonamici (2011), a segurança pública, diante de sua inclusão no artigo 5º da Constituição Federal, seria direito fundamental de primeira geração, enquanto a previsão no artigo 6º refletiria direito social, mormente de segunda geração. Além disso, Valter Foletto Santin (citado por Buonamici, 2011) aponta que a segurança seria inegável direito difuso.

Segundo Ávila (2014, p. 161-162):

> A mutação do Estado de mero "guarda-noturno" em suprema entidade fornecedora de bens e serviços públicos criou novas tensões dialéticas na concretização do direito à segurança pública. Enquanto no paradigma liberal o Estado apenas evita agressões de terceiros (e de si mesmo), no Estado social, além de evitar tais agressões, o Estado passa a ter uma responsabilidade acentuada em fornecer condições efetivas de fruição dos direitos, ou seja, trata-se de um Estado comprometido com a promoção do bem estar da sociedade, especialmente com os setores mais desfavorecidos, mas ainda sem resvalar no risco absolutista de promover o bem público sem quaisquer limites. [...]
>
> [...] No Estado liberal, a atividade de promoção da segurança pública aparece como uma atividade de sobrevivência do próprio Estado, já que, em última análise, essa é a atividade que fundamentou o surgimento do Estado (como visto em Hobbes) e, portanto, desempenhar bem essa atividade se torna uma questão de defesa da própria necessidade da existência do Estado. Todavia, o Estado social reconhece que o valor da segurança pública não será algo que aparecerá por geração espontânea, antes necessita de uma direção estatal para sua configuração. Essas perspectivas sociais possuem especial interligação com uma política criminal global de promoção de segurança jurídica, não apenas através dos tradicionais instrumentos do direito penal, mas também através de outras estratégias de organização da vida social que diminuam a probabilidade de ocorrência de fenômenos criminosos (e, especificamente quanto à realidade brasileira, a concretização efetiva de políticas de inclusão social assuma uma dimensão especialmente relevante).

Por esse prisma, percebe-se que o direito fundamental à segurança pública é multigeracional, pois, tratando-se de verdadeiro pré-requisito à constituição do Estado, ele esteve presente durante a evolução do Estado moderno para o Estado contemporâneo, de modo que, ante tal evolução, referido direito também foi se alterando e adquirindo novas facetas.

Em uma primeira toada, como direito de primeira geração, o direito à segurança pública voltava-se ao indivíduo, notadamente para lhe garantir liberdade a fim de exercer sua autonomia privada, vedando atos atentatórios a esses direitos de primeira geração, além também de representar uma faceta negativa, no sentido de evitar arbítrios estatais.

Assim, nessa perspectiva de primeira geração, o direito à segurança pública se encontra presente no art. 5º da Constituição Federal (Buonamici, 2011), que elenca diversos direitos fundamentais de índole primordialmente individual e estabelece, inclusive, diversas garantias aos indivíduos em face da persecução criminal, buscando o equilíbrio anteriormente mencionado.

Essa perspectiva, apesar do aspecto histórico-evolutivo, é limitada e não atende às demandas da sociedade contemporânea quanto à segurança pública, que não se contenta com posturas passivas e reativas, mas clama por ações positivas do Estado. Nesse sentido pontuam Azevedo e Basso (2008, p. 28):

> Por tudo o que foi visto, tem-se que o direito fundamental à segurança pessoal faz parte da primeira dimensão dos direitos fundamentais, vinculado que está à integridade física, à liberdade pessoal, etc. A segurança pública, por sua vez, pode ser concebida como a dimensão pública da segurança pessoal e, assim como a habitação, saúde, etc., necessita de um agir Estatal, estando situada, por isso, na segunda dimensão dos direitos fundamentais.

Cuidando-se de direito fundamental, a perspectiva de segunda geração do direito à segurança pública se encontra no artigo 6º da Constituição Federal, como mencionado anteriormente (Buonamici, 2011).

Nesse contexto, o direito à segurança não foca mais apenas no indivíduo, mas na resolução de problemas sociais, demandando agir do Estado, inclusive em interação com outros direitos sociais, como educação, saúde, habitação, que se encontram correlacionados com a segurança pública.

A segurança pública aqui assume dimensão de política pública concreta, gerando ao particular direito subjetivo do recebimento dos serviços respectivos (Buonamici, 2011). Como consequência de ser direito social, a segurança se encaixa na cláusula da proibição de retrocesso, impedindo situações que gerem perda de proteção (Buonamici, 2011).

Embora a doutrina majoritária limite-se a separar a segurança pública entre o direito individual, de primeira geração, e o direito social, de segunda geração, entende-se que, no arcabouço normativo constitucional, há espaço para consideração de uma perspectiva da segurança pública como direito fundamental de terceira geração.

Essa perspectiva difusa se encontra prevista no artigo 144 da Constituição Federal (Brasil, 1988, título V, cap. III, artigo 144), ao prever que a "segurança pública, dever do Estado, direito e responsabilidade de todos, é exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio".

Como se percebe, o artigo assume ares difusos, denotando que a segurança não é apenas direito, mas responsabilidade de todos, veiculando o caráter fraternal que deve ser adotado na seara, à semelhança, por exemplo, da redação do artigo 225 da Constituição Federal (Brasil, 1988), de índole marcadamente difusa.

Ao assentar a dimensão de terceira geração do direito à segurança pública, nota-se a ausência de titularidade definida do direito, que passa a ser de uma coletividade indeterminável, porque todos podem ser, em algum momento, vítimas de um crime.

Essa perspectiva coletiva já é incorporada por Ávila (2016, p. 173-174):

> Outra perspectiva do direito à segurança ocorre em um nível coletivo, sem a existência de uma possível vítima já individualizada numa situação concreta de perigo. Nessa outra perspectiva, todos os integrantes da coletividade são possíveis titulares desse direito, já que todos são potenciais vítimas de possíveis violações de seus direitos e, portanto, têm a expectativa de que o Estado estruture uma atividade de segurança pública que diminua a probabilidade de serem vítimas desses crimes ou que, caso eles ocorram, o Estado esteja a postos para intervir e restabelecer a normalidade da fruição dos direitos. Nessa perspectiva coletiva (transindividual), o direito à segurança não corresponde ao direito a uma ação concreta e específica, mas o direito à existência de uma política pública de segurança que seja minimamente eficiente para assegurar a legítima expectativa de proteção dos direitos dos cidadãos. Ele é indivisível, pois a expectativa de ter as garantias mínimas de proteção para viver e se desenvolver de forma digna não pode ser fracionada, pelo que esse direito à segurança não pertence a ninguém em particular, mas a todos em geral, pelo que é um direito difuso, ou seja, é admissível se gozo individual apenas na medida em que todos os integrantes da coletividade também estejam a dele usufruir. Em regra, a atividade de prevenção criminal de estruturação da polícia para estar minimamente apta a reagir com eficiência diante do crime configura-se num direito à segurança numa perspectiva coletiva.

A perspectiva difusa e coletiva ganha relevo em uma sociedade de risco, que enfrenta altos índices de criminalidade e em que a ação humana desponta perigos difusos, demandando atuação do Estado para prevenção de tais riscos, direcionando a segurança ao futuro (Azevedo e Basso, 2008).

Em tal seara, vai-se além da política pública voltada a fornecer prestações positivas aos indivíduos em solução aos problemas existentes, para se incorporar uma perspectiva não apenas focada no problema, mas no futuro, em proteção a situações vindouras. A postura difusa, exatamente por não comportar a titularidade individualizada, reclama soluções estruturantes, com análise global da situação em vistas à formação de arranjos eficientes não apenas à persecução penal, mas à própria redução da criminalidade.

Sobre o tema, mostra-se pertinente colacionar lição de Moraes (2016, p. 276):

> Ao se considerar a segurança pública, tanto como bem puramente difuso, quanto como bem difuso que demanda proteção jurídico-penal, substitui-se a percepção de que somente uma parcela das pessoas atingidas pela criminalidade seriam sujeitos passivos dos crimes e tem-se, por lógica, a ideia de que todos indistintamente são tanto titulares desse interesse, quanto potenciais vítimas.

Logo, enquanto, em primeira geração, o direito à segurança pública reflete o direito individual de ação estatal após a ocorrência do risco, em segunda geração trata-se do direito social de montagem da política pública de segurança que será exigível individualmente por quem porventura seja vítima de crime, ao passo que, em terceira geração, o direito à segurança pública se relaciona com medidas de índole coletiva e difusa, que superam as perspectivas individuais e reclamam ações efetivas e estruturantes para a sociedade como um todo.

É importante relembrar, contudo, que as gerações não se superam, mas se complementam, o que significa, dessa forma, que todas essas perspectivas de segurança pública convivem simultaneamente.

2.3. DIREITO HUMANO

Os direitos humanos podem ser caracterizados como o "conjunto de direitos considerado indispensável para uma vida humana pautada na liberdade, igualdade e dignidade" (Ramos, 2023, p. 19).

Boa parte da doutrina aponta que a diferença com os direitos fundamentais residiria na positivação, porquanto estes seriam exigíveis no âmbito interno, como visto no tópico anterior, ao passo que os direitos humanos, atualmente, estariam previstos no plano do Direito Internacional (Fernandes, 2018).

Essa distinção é adotada por Ingo Sarlet (2022, p. 138):

> De acordo com o critério aqui adotado, o termo "direitos fundamentais" se aplica àqueles direitos (em geral atribuídos à pessoa humana) reconhecidos e positivados na esfera do direito constitucional positivo de determinado Estado, ao passo que a expressão "direitos humanos" guarda relação com os documentos de direito internacional, por referir-se àquelas posições jurídicas que se reconhecem ao ser humano como tal, independentemente de sua vinculação com determinada ordem constitucional, e que, portanto, aspiram à validade universal, para todos os povos e em todos os lugares, de tal sorte que revelam um caráter supranacional (internacional) e universal.

A internacionalização dos direitos humanos decorreu no pós-segunda Guerra como reação aos horrores praticados durante o regime nazista, com a criação da Organização das Nações Unidas em 1945, cuja carta de constituição aborda, em diversos pontos, a temática dos direitos humanos (Ramos, 2023). O marco internacional sobre a matéria advém em 1948, com a edição da Declaração Universal dos Direitos Humanos (DUDH), sob a forma Resolução, pela Assembleia Geral da Organização das Nações Unidas (Ramos, 2023).

O reconhecimento de distinção entre direitos fundamentais e direitos humanos não significa, todavia, afastar a íntima correlação existente entre eles, até porque existe, atualmente, um processo de harmonização, em que os textos constitucionais se aproximam dos documentos internacionais. Sobre o tema, bem expôs Ingo Sarlet (2022, p. 139):

> Em face dessas constatações, verifica-se que as expressões "direitos fundamentais" e "direitos humanos", em que pese sua habitual utilização como sinônimas, se reportam, por várias razões, a significados em parte distintos. No mínimo, para os que preferem a expressão "direitos humanos", há que referir – sob pena de se correr o risco de gerar uma série de equívocos – se eles estão sendo analisados pelo prisma do direito internacional ou na sua dimensão constitucional positiva. Reconhecer a diferença, contudo, não

> significa desconsiderar a íntima relação entre os direitos humanos e os direitos fundamentais, uma vez que a maior parte das constituições do segundo pós-guerra se inspirou tanto na Declaração Universal de 1948 quanto nos diversos documentos internacionais e regionais que a sucederam, de tal sorte que – no que diz com o conteúdo das declarações internacionais e dos textos constitucionais – está ocorrendo um processo de aproximação e harmonização, rumo ao que já está sendo denominado (não exclusivamente – embora principalmente – no campo dos direitos humanos e fundamentais) um direito constitucional internacional.

No caso brasileiro, esse processo de harmonização é inegável, uma vez que a Constituição Federal conta com abertura material, em seu artigo 5º, §2º, para reconhecimento de outros direitos e garantias decorrentes "dos tratados internacionais em que a República Federativa do Brasil seja parte" (Brasil, 1988, título II, cap. I, artigo 5º, §2º), sendo que, nas relações internacionais, o Brasil se rege, dentre outros, pela "prevalência dos direitos humanos" (Brasil, 1988, título I, artigo 4º, II).

Presente a premissa de que os direitos humanos são extraídos, atualmente, a partir de documentos firmados no âmbito internacional, cumpre analisar o embasamento internacionalista/convencional à segurança pública.

Como visto anteriormente, a internacionalização dos direitos humanos ocorreu no cenário pós segunda guerra mundial, em um mundo ainda em choque dos horrores experimentados no período, em que as vidas humanas foram submetidas à barbárie. Consequentemente, há de se imaginar que a segurança pública, como forma de autopreservação humana, tenha sido incorporada como valor a ser observado.

Em tal toada, já na Declaração Universal dos Direitos do Homem e do Cidadão aparece, no artigo 3º, que "toda pessoa tem direito à vida, à liberdade e à segurança pessoal" (Barreto e Borges, 2018, p. 65)

Embora exista posicionamento de que a segurança pessoal mencionada no documento reflita apenas garantia contra arbitrariedade estatal (Erthal, 2020), naquela perspectiva negativa de primeira geração anteriormente abordada, reputa-se mais adequada a interpretação que se trata do "direito de viver sem medo, protegido pela solidariedade e livre de agressões" (Barreto e Borges, 2018, p. 77).

Em decorrência, cabe ao Poder Público promover o direito à segurança, garantindo o exercício dos demais direitos, até porque, sem segurança, o próprio poder político fica comprometido (Barreto e Borges, 2018).

Percebe-se, então, que, desde o documento inaugural dos direitos humanos na seara internacional, já há previsão do direito à segurança.

Aliás, Buonamici (2011) assevera que, com o findar de uma das guerras mais sangrentas da humanidade, a Declaração Universal de Direitos Humanos espelha o direito à segurança pública não apenas pela lógica necessidade de se preservar os demais direitos, mas como um inegável direito difuso, corroborando o apontado anteriormente, no sentido de que a leitura de mencionado direito não pode ficar apenas na perspectiva negativa de primeira geração.

Sobre a força normativa da Declaração Universal de Direitos Humanos, o tema é controvertido, havendo três correntes: a primeira a considera vinculante, por se tratar de interpretação autêntica do termo "direitos humanos" presente na Carta da ONU; a segunda também a considera vinculante, mas por espelhar costume internacional sobre o tema; e, por fim, a terceira entende que se trata de *soft law*, sem força de tratado, destinada apenas a orientar a ação futura dos Estados (Ramos, 2023).

Segundo sua concepção, Ramos (2023, p. 28) reputa que "parte da DUDH é entendida como espelho do costume internacional de proteção de direitos humanos, em especial quanto aos direitos à integridade física, igualdade e devido processo legal". Logo, por esse prisma, o direito à segurança, decorrente do direito à integridade física, deteria eficácia vinculante às nações.

Nada obstante, dada a controvérsia existente acerca da normatividade da Declaração, foram editados o Pacto Internacional sobre Direitos Civis e Políticas (PIDCP) e o Pacto Internacional sobre Direitos Econômicos, Sociais e Culturais (PIDESC), de modo a trazer os direitos da DUDH para tratados internacionais, detalhando o tema e afastando divergência sobre a eficácia normativa (Ramos, 2023).

Quanto ao direito à segurança, ele aparece no artigo 9º do PIDCP, com detalhamento do seu conteúdo, que segue a linha de evitar arbitrariedades estatais, no sentido de direito negativo de primeira geração (Brasil, 1992a).

No âmbito interamericano, por sua vez, a previsão do artigo 7º do Pacto de São José da Costa Rica segue a linha do artigo 9º do PIDCP, abordando a segurança pessoal sob prisma de garantias contra ingerências estatais (Brasil, 1992a, 1992b).

Apesar de isso, à primeira vista, aparentar ser indicativo de que, na seara internacional, o direito à segurança se resumiria à proteção contra arbitrariedades estatais, não é tal conclusão que se extrai da jurisprudência especializada sobre a matéria.

Em realidade, tanto a Corte Europeia quanto a Corte Interamericana de Direitos Humanos reconhecem a existência de obrigações processuais penais positivas dos Estados, que devem atuar na proteção de direitos humanos/fundamentais, punindo as violações (Fischer e Pereira, 2023).

A ideia, portanto, de que o direito à segurança se cingiria à proteção contra arbitrariedades estatais se encontra ultrapassada, porque a proteção de direitos humanos depende da "adoção de ações positivas direcionadas a prevenir e sancionar com eficiência as ofensas que eventualmente lhes podem ser direcionadas, buscando-se sempre um equilíbrio nas relações entre todos os direitos e deveres fundamentais" (Fischer e Pereira, 2023, p. 245).

Nessa senda, tanto a Convenção Europeia de Direitos Humanos quanto a Convenção Americana (Pacto de São José) possuem diversas obrigações positivas, que, segundo decisões das Cortes respectivas, decorrem, em geral, da própria imposição aos Estados-Partes do "dever de respeito aos direitos fundamentais afirmados nas convenções" (Fischer e Pereira, 2023, p. 249).

O Superior Tribunal de Justiça assentou, inclusive, que qualquer homicídio doloso "representa grave violação ao maior e mais importante de todos os direitos do ser humano, que é o direito à vida, previsto no art. 4º, nº 1, da Convenção Americana sobre Direitos Humanos, da qual o Brasil é signatário por força do Decreto nº 678, de 6/11/1992*"* (Brasil, 2015, IDC n. 1/PA, relator Ministro Arnaldo Esteves Lima, Terceira Seção, julgado em 8/6/2005, DJ de 10/10/2005, p. 217).

Inclusive, consoante assenta Oliveira (2022, p. 163), os deveres de proteção impostos ao Estado no plano interno (leia-se decorrentes do direito fundamental à segurança pública) "encontram perfeita correspondência no plano dos direitos humanos na doutrina das obrigações positivas (*obligaciones positivas*), de acordo com a terminologia adotada pela própria Corte Interamericana de Direitos Humanos".

Tais obrigações impõem ao Estado o dever de "adotar efetivas medidas de prevenção de ofensas a direitos humanos, de maneira a evitar a ocorrência de violações dessa natureza em desfavor de seus jurisdicionados" (Oliveira, 2022, p. 165).

Trata-se, então, do reconhecimento de um efetivo direito humano à segurança pública.

Especificamente em relação à Convenção Americana, esse reconhecimento pode ser extraído, conforme Oliveira (2022), dos seguintes dispositivos: artigo 1.1, que determina aos Estados o respeito aos direitos e liberdades reconhecidos no documento; artigo 8.1, que prevê

a possibilidade de participação de toda a pessoa perante juiz para determinação de seus direitos (aplicado também a familiares de vítima de desaparecimento, consoante decisão no caso Blake vs. Guatemala); e artigo 25.1, que dispõe que toda a pessoa deve ter direito a um recurso simples, rápido e efetivo para proteção contra atos violadores de seus direitos.

Está expresso no artigo 25.1 o direito à proteção judicial, que, conjugado com as garantias judiciais do artigo 8.1, leva a Corte Interamericana a reconhecer violações de direitos da vítima pela inação do Estado, quando este se omite na condução de uma investigação séria, imparcial e eficiente de delitos (Oliveira, 2022).

Aliás, é interessante salientar que, segundo Oliveira (2022), o artigo 25.1 irradia efeitos também para os ordenamentos internos e impõe proteção a outros direitos fundamentais previstos na legislação interna que, porventura, não estejam alcançados no rol tipificado na Convenção Interamericana. Assim, existe evidente harmonização do direito fundamental à segurança pública explicado no tópico anterior com o direito humano à segurança pública, de modo que a temática deve ser enfrentada de forma una para adequada compreensão do conteúdo de tal direito.

Portanto, o direito à segurança não se resume a uma perspectiva negativa de primeira geração, mas assume contornos positivos e demanda agir estatal, de modo a tutelar a coletividade, transbordando para as segunda e terceira gerações.

2.4. SITUAÇÃO BRASIL

Consagrada na seara internacional a existência do direito humano à segurança pública, cumpre avaliar a aplicação de tal previsão ao Brasil. Para tanto, serão analisadas as condenações do Brasil pela Corte Interamericana de Direitos Humanos, órgão cuja competência jurisdicional foi reconhecida pelo país.

Sobre o tema, é interessante relembrar colocação de Antônio Augusto Cançado Trindade, no sentido de que o papel de um Tribunal de Direitos Humanos, como a Corte Interamericana, não é apenas decidir casos, mas explicar o que é o direito (citado por Oliveira, 2022).

Ademais, “o Brasil é pródigo em reiteradas condenações internacionais por descumprimento a deveres convencionais de proteção a direitos humanos, invariavelmente em

virtude do não atendimento das suas obrigações positivas em matéria penal" (Oliveira, 2022, p. 200), de modo que a análise da jurisprudência da Corte Interamericana se faz fundamental para compreender tanto o escopo do direito humano à segurança pública aplicada à realidade brasileira quanto os pontos falhos do Estado na tutela de tal direito.

Inclusive, é pertinente lembrar que os entendimentos firmados na Corte Interamericana de Direitos Humanos devem ser observados pelos juízes pátrios (vide Recomendação n. 123/22 do CNJ) e que a Corte não julga responsabilidade individual, mas, sim, a responsabilidade estatal por descumprimento das normas internacionais de direitos humanos (Fischer e Pereira, 2023).

Consignado tal ponto, passa-se à análise dos casos, sem ser possível, todavia, adentrar em minúcias de cada caso, dados o escopo e a limitação do presente trabalho.

O Brasil, até a data da conclusão deste trabalho[1], foi condenado treze vezes pela Corte Interamericana de Direitos Humanos.

A primeira condenação brasileira ocorre no caso Damião Ximenes Lopes, cujo contexto revolve a morte de Damião, pessoa com deficiência mental, decorrente de suposta tortura experimentada durante internação na casa de Repouso Guararapes em Sobral/CE no ano de 1999 (Fischer e Pereira, 2023).

No caso, a Corte reconheceu a falha do Estado brasileiro em investigar e punir a morte possivelmente decorrente de tortura vivenciada por Damião Ximenes Lopes, inclusive porque ele estava em instituição destinada à prestação de um serviço público de saúde, apontando "violação dos direitos às garantias judiciais e à proteção judicial consagrados nos artigos 8.1 e 25.1 da Convenção Americana, em relação com o artigo 1.1 desse mesmo tratado, em detrimento [...]" de familiares da vítima (Corte Interamericana de Direitos Humanos, 2006).

Na oportunidade, a Corte assentou o seguinte (Corte Interamericana de Direitos Humanos, 2006, p. 65-66):

> 193. O recurso efetivo do artigo 25 da Convenção deve tramitar-se conforme as normas do devido processo estabelecidas no artigo 8 desse tratado, do qual se depreende que as vítimas das violações dos direitos humanos, ou seus familiares, devem dispor de amplas possibilidades de ser ouvidos e de atuar

1 Embora se aguarde a publicação da sentença do décimo quarto caso: Caso Leite de Souza e Outros, julgado em 04 de julho de 2024.

> nos respectivos processos, tanto na tentativa de esclarecer os fatos e punir os responsáveis, quanto na busca de uma devida reparação.
>
> 194. Em resposta aos tratamentos cruéis, desumanos e degradantes a que foi submetido o senhor Damião Ximenes Lopes, e a sua posterior morte, o primeiro recurso que cabia ao Estado ter proporcionado era uma investigação efetiva e um processo judicial realizado de acordo com os requisitos do artigo 8 da Convenção, com vistas ao esclarecimento dos fatos, à punição dos responsáveis e à concessão de compensação adequada.
>
> 195. O artigo 8.1 da Convenção dispõe, como um dos elementos do devido processo, que os tribunais decidam os casos submetidos ao seu conhecimento em prazo razoável. A razoabilidade do prazo deve ser apreciada em relação com a duração total do processo penal. Em matéria penal este prazo começa quando se apresenta o primeiro ato de procedimento contra determinada pessoa como provável responsável por certo delito e termina quando se profere sentença definitiva e firme.
>
> [...]
>
> Neste ponto é importante ressaltar que o Ministério Público é um órgão do Estado, motivo por que suas ações e omissões podem comprometer a responsabilidade internacional desse mesmo Estado.

Percebe-se, então, que o caso aborda a ineficiência do Estado em investigar e punir a morte de uma pessoa com deficiência que estava internada em instituição prestadora de serviço de saúde e provavelmente lá sofrera tortura.

A segunda e a terceira condenações do Brasil, isto é, Caso Escher e outros e Caso Garibaldi, ambas datadas de 2009, revolvem o mesmo contexto fático, consistente em disputa agrária no Estado do Paraná (Ramos, 2023).

O Caso Escher decorre da "interceptação, gravação e divulgação das conversas telefônicas de vários indivíduos de movimentos sociais de modo totalmente indevido de acordo com a própria lei brasileira" (Ramos, 2023, p. 277), feitas pela Polícia Militar sem participação do Ministério Público e sem investigação formal, apenas para controle do movimento sem-terra, que estava em choque com fazendeiros da região. A violação ocorreu pela falta da devida apuração sobre os responsáveis pela divulgação das interceptações ilegais, assentando a Corte que "a falta de resposta estatal é um elemento determinante ao analisar se foram respeitados os artigos 8.1 e 25.1 da Convenção Americana, pois tem relação direta com o princípio da efetividade e deve caracterizar o desenvolvimento de tais investigações" (Corte Interamericana de Direitos Humanos, 2009a, p. 62). A Corte reputou que "as autoridades estatais não atuaram

com a devida diligência nem conforme com as previsões consagradas nos artigos mencionados concernentes ao dever de investigar" (Corte Interamericana de Direitos Humanos, 2009a, p. 62)

O Caso Garibaldi revolve o homicídio de Sétimo Garibaldi em 27/11/1998, durante operação extrajudicial de despejo de famílias sem-terra ocupantes de fazenda em Município do Paraná; na oportunidade, um grupo de aproximadamente vinte homens armados e encapuzados chegaram ao local efetuando disparos para realizar a desocupação forçada, sendo que um dos disparos acabou atingindo a vítima, que faleceu (Fischer e Pereira, 2023).

Embora os fatos sejam anteriores ao reconhecimento da competência contenciosa da Corte pelo Brasil, em dezembro de 1998, foi possível analisar a condução da investigação pelo Estado (Fischer e Pereira, 2023). E, no caso, a Corte entendeu flagrante o descumprimento das obrigações processuais penais positivas pelo Estado, que não conduziu investigação profunda e eficaz, dentro de um prazo razoável. Assim, reputou que "o Estado violou os direitos às garantias e à proteção judiciais previstos nos artigos 8.1 e 25.1 da Convenção Americana, em relação com o artigo 1.1", em relação aos familiares da vítima (Corte Interamericana de Direitos Humanos, 2009b, p. 39).

Ambos os casos acima envolvem, como visto, ineficiência estatal em averiguar e punir violações contra integrantes de movimentos sociais, de modo a permitir a impunidade de tais violações em âmbito interno.

Em seguida, analisam-se os casos Gomes Lund ("Guerrilha do Araguaia") e Herzog, pois ambos tratam de fatos ocorridos durante o regime de ditadura militar no país. Por consequência, os fatos em si escapam da jurisdição contenciosa da Corte, reconhecida a partir de dezembro de 1998, o que não impede, contudo, a análise da conduta estatal quanto à situação após tal reconhecimento.

O Caso Gomes Lund revolvia "detenção arbitrária, tortura e desaparecimento forçado de 70 pessoas, que teria sido resultado de operações do Exército brasileiro, fatos ocorridos entre 1972 e 1975, com a finalidade de erradicar a 'Guerrilha do Araguaia'" (Fischer e Pereira, 2023, p. 211). Já o Caso Herzog apurou a "detenção arbitrária, tortura e a morte o jornalista Vladimir Herzog, ocorridas em 25 de outubro de 1975, durante a ditadura militar" (Fischer e Pereira, 2023, p. 227).

Ambos os casos têm como pano de fundo a Lei n. 6.683/79 (Lei de Anistia), que concede anistia aos "crimes políticos ou conexos com estes", "no período compreendido entre 02 de setembro de 1961 e 15 de agosto de 1979", o que resulta, na realidade, em impunidade aos

crimes ocorridos na época pelos agentes do governo, diante da extensão abrangente do §1º do artigo 1º da referida Lei, que prevê que os crimes conexos são "crimes de qualquer natureza relacionados com crimes políticos ou praticados por motivação política" (Brasil, 1979, artigo 1º, §1º). É interessante observar que o STF reconheceu a compatibilidade da mencionada Lei com a Constituição Federal por meio do julgamento da ADPF 153 (Fischer e Pereira, 2023).

Nada obstante, a Corte Interamericana, fundada em precedentes da Corte Europeia de Direitos Humanos, assinalou que "crimes, como a tortura, que impliquem graves violações de direitos humanos sejam imprescritíveis e não passíveis de anistias e similares" (Fischer e Pereira, 2023, p. 214), de modo que a Lei de Anistia não poderia representar obstáculo à punição dos atos violadores de Direitos Humanos.

Esse ponto é extremamente importante para reforçar que o direito à segurança pública, inclusive na seara internacional, não se resume a apenas uma faceta negativa de primeira geração, contra arbitrariedades estatais, mas revolve obrigações processuais positivas de punição às violações de direitos humanos, até mesmo pelo reconhecimento de crimes imprescritíveis (o que estaria em desconformidade com previsão constitucional brasileira, que, no ponto, seria inconvencional).

Logo, as normativas de direitos humanos demandam a punição de atos violadores de direitos humanos, que não podem ser abonados pelo Estado, sob pena de responsabilização internacional.

Assim, pela falta de investigação e punição dos mencionados crimes, praticados por motivação política contra opositores ao regime militar, a Corte Interamericana de Direitos Humanos reconheceu a responsabilidade estatal brasileira por violação aos direitos de acesso à justiça, assentando que a punição a tais delitos decorre de normas *jus cogens* (ou seja, obrigatórias de direito internacional).

Mais uma vez, então, a condenação do Brasil abarca cenário de impunidade, decorrente, nessa hipótese, de crimes violadores de direitos humanos contra opositores políticos do regime que deixaram de ser investigados e punidos, descumprindo-se obrigações processuais penais positivas (Fischer e Pereira, 2023) e violando, consequentemente, o direito à segurança, em sua faceta positiva.

Em seguida, analisa-se o Caso Favela Nova Brasília, também decorrente de violência praticada por agentes estatais que deixou de ser punida. No caso, trata-se de duas operações policiais realizadas na Favela Nova Brasília, no Rio de Janeiro, nos anos de 1994 e 1995, que

deixaram, cada uma, 13 mortos, sob o pretexto de os vitimados terem resistido à prisão, sendo que, na primeira incursão, dentre os mortos, havia 4 crianças, além do relato de prática de violência sexual contra três jovens (Fischer e Pereira, 2023). Os crimes, em si, escapam, como visto anteriormente, da competência contenciosa da Corte, que, todavia, pode analisar as medidas tomadas pelo Estado a partir de dezembro de 1998 (Fischer e Pereira, 2023).

A Corte ponderou que, conforme reiterada jurisprudência, os Estados "são obrigados a oferecer recursos judiciais efetivos às vítimas de violações de direitos humanos (artigo 25), recursos cuja tramitação observará as regras do devido processo legal (artigo 8.1)" (Corte Interamericana de Direitos Humanos, 2017, p. 44), ressaltando que esse "dever de 'garantir' os direitos implica a obrigação positiva de adoção, por parte do Estado, de uma série de condutas, dependendo do direito substantivo específico de que se trate*"* (Corte Interamericana de Direitos Humanos, 2017, p. 45).

Em casos de execuções extrajudiciais, a Corte apontou o dever de uma investigação efetiva, que se "torna mais intenso quando nele estão ou podem estar implicados agentes estatais" (Corte Interamericana de Direitos Humanos, 2017, p. 45). Assentou-se, inclusive, que, em tais hipóteses, "o órgão investigador seja independente dos funcionários envolvidos no incidente. Essa independência implica a ausência de relação institucional ou hierárquica, bem como sua independência na prática" (Corte Interamericana de Direitos Humanos, 2017, p. 47).

Além disso, pontuou-se os seguintes critérios para condução de uma investigação efetiva: "i) a adequação das medidas de investigação; ii) sua celeridade; e iii) a participação da família da pessoa morta e iv) a independência da investigação*"* (Corte Interamericana de Direitos Humanos, 2017, p. 48).

No caso, contudo, não houve a condução de investigação efetiva e imparcial, assim como a classificação do ocorrido como "autos de resistência à prisão" impactou todo o procedimento, de modo que medidas investigativas efetivas deixassem de ser adotadas, para culpabilizar a própria vítima por sua morte (Corte Interamericana de Direitos Humanos, 2017).

Assim, reconheceu-se o descumprimento de dispositivos de direitos humanos pelo Brasil.

Logo, nesse caso, tratava-se de violência contra moradores de periferia praticada por agentes estatais que deixou de ser investigada e punida. É interessante observar que a própria Corte assinala a relevância da participação dos familiares da vítima na investigação, o que, certamente, se cuida de ponto para evolução no processo penal brasileiro, arraigado na

perspectiva de segurança pública como direito negativo de primeira geração, em que a vítima é muitas vezes tida como mero objeto do processo.

O próximo caso a ser analisado revolve a omissão do Brasil na prevenção e repressão de situações contemporâneas de escravidão e o desaparecimento de dois adolescentes (Ramos, 2023). Trata-se do Caso Fazenda Brasil Verde, relativo a uma fazenda localizada no Estado do Pará, em que se provou (Ramos, 2023, p. 278):

> [...] contexto de captação ou aliciamento de trabalhadores rurais por meio de fraude, enganos e falsas promessas para fazendas no norte do Brasil. Também ficou provada a situação de discriminação estrutural histórica em razão da vulnerabilidade dos trabalhadores rurais (a maioria analfabetos), o que o Brasil deveria ter levado em conta na prevenção e repressão das práticas escravagistas.

Novamente o Brasil descumpriu suas obrigações processuais penais positivas e foi condenado pela Corte, assentando-se que a proibição da escravidão é norma *jus cogens* e, portanto, o crime correlato é imprescritível (Fischer e Pereira, 2023).

Mais uma vez se sinalizou hipótese de imprescritibilidade não elencada na Constituição Federal. Além disso, abordou-se o tema da vulnerabilidade, a facilitar a vitimização de determinados grupos, a reforçar a necessidade de atuação estatal.

Especialmente, em citação à OIT, a Corte sinalizou o seguinte (Corte Interamericana de Direitos Humanos, 2016, p. 89): “a pobreza, nesse sentido, é o principal fator da escravidão contemporânea no Brasil, por aumentar a vulnerabilidade de significativa parcela da população, tornando-a presa fácil dos aliciadores para o trabalho escravo”.

O próximo caso a ser analisado é o Caso Povo Indígena Xucuru, referente à demora no “processo administrativo de reconhecimento, titulação, demarcação e delimitação [...]” de terras e territórios ancestrais indígenas (Ramos, 2023, p. 279), além da demora na “desintrusão total dessas terras e territórios, para que o referido povo indígena pudesse exercer pacificamente esse direito” (Fischer e Pereira, 2023, p. 225).

Apesar de, no caso em questão, não terem sido constatadas efetivas violações a obrigações processuais penais positivas, até porque a Corte se debruçou mais sobre a violação ao direito de demarcação da terra indígena, houve menção à morte de três líderes indígenas e um servidor da FUNAI no contexto apreciado (Fischer e Pereira, 2023). Ramos (2023, p. 280)

aponta que as mortes não foram avaliadas por serem anteriores ao reconhecimento da competência jurisdicional da Corte, mas foram importantes “para entender o contexto turbulento do conflito nas demarcações e procedeu à análise das violações em razão dos fatos posteriores à aceitação da sua competência contenciosa”.

O caso a seguir se trata do Caso Empregados da Fábrica de Fogos de Santo Antônio de Jesus, referente a “violações de direitos humanos decorrentes da explosão da fábrica de fogos de artifício em Santo Antônio de Jesus/BA que causou a morte de 60 pessoas e lesão de outras 6, em 11-12-1998” (Ramos, 2023, p. 281).

Cuida-se de situação mais uma vez relativa à pobreza da comunidade, cujos integrantes se submeteram a trabalho de alto risco em condições precárias, sem mínima segurança, por salários baixos, havendo conivência dos órgãos públicos com a situação (Ramos, 2023).

Nesse caso, também não houve punição aos responsáveis, e a Corte reiterou sua jurisprudência ao assentar que “a demora de quase 22 anos sem uma decisão definitiva configurou uma falta de razoabilidade no prazo por parte do Estado para levar a cabo o processo penal*”* (Corte Interamericana de Direitos Humanos, 2020, p. 65).

Novamente se estabeleceu a correlação entre os artigos 25, 8 e 1.1 para fundamentar que o devido processo abarca também os interesses da vítima, reforçando, então, as obrigações processuais penais positivas (Fischer e Pereira, 2023).

Segue-se, agora, à análise do Caso Barbosa Souza que revolve “a morte de Márcia Barbosa de Souza causada por um ex-deputado estadual*”* (Ramos, 2023, p. 281), em junho de 1998. O processo penal correlato ao homicídio teve paralisações em razão do foro por prerrogativa de função sustentado pelo réu, que, à época, devido à redação constitucional vigente, permitia a paralisação do procedimento criminal por falta de autorização da respectiva casa legislativa (Fischer e Pereira, 2023). O autor dos fatos acabou morrendo durante o curso da ação penal, sem que sofresse qualquer punição.

A Corte, apesar de assinalar a importância da imunidade parlamentar, destacou que ela não pode funcionar como “obstáculo para a devida e pronta investigação de casos de violações de direitos humanos” (Ramos, 2023, p. 281), ressaltando que o “Estado falhou na investigação de outros envolvidos no feminicídio, mostrando falta de perspectiva de gênero na investigação criminal” (Ramos, 2023, p. 281).

Assim, a “ineficácia judicial perante situações concretas de violência contra a mulher gera um ambiente de impunidade, apto a incentiva a repetição de fato de violência em geral”

(Fischer e Pereira, 2023, p. 237). A Corte inclusive assentou que há um alcance adicional da obrigação de melhor investigar "quando se tratar de crime cometido em condições gerais de violência contra mulheres" (Fischer e Pereira, 2023, p. 238).

Percebe-se, mais uma vez, um caso de omissão do Estado na punição de crimes praticados contra pessoa em situação de vulnerabilidade, aqui em razão do gênero. Novamente a Corte assentou dever especial de proteção em tais situações, demandando uma obrigação adicional quanto ao dever de investigar.

Há, ainda, a condenação brasileira no Caso Sales Pimenta, relativo à *"*situação de impunidade dos atos referentes à morte de Gabriel Sales Pimenta, defensor dos direitos dos trabalhadores rurais, ocorrida em 1982 no Estado do Pará" (Ramos, 2023, p. 282).

A Corte assinalou a existência de ambiente de impunidade, que dava a margem à reiteração de atos semelhantes, exatamente porque o Brasil descumpria o dever de investigação e punição, que se trata de dever jurídico próprio e não mero formalismo sem qualquer chance de êxito (Fischer e Pereira, 2023).

Sobre o caso, também havia uma especial obrigação de investigar e punir, pois agressões contra defensores de direitos humanos gera um efeito amedrontador (*chilling effect*), sobretudo em situações de impunidade (Fischer e Pereira, 2023).

Logo, o Brasil novamente violou os artigos 81., 25 e 1.1 da Convenção Interamericana de Direitos Humanos.

Recentemente, no ano de 2023, o Brasil foi condenado em outros dois casos: Tavares Pereira e outros, e Honorato e outros.

Segundo Resumo Oficial da Corte Interamericana, o Caso Tavares Pereira e outros consistiu no seguinte (Corte Interamericana de Direitos Humanos, 2023b):

> Em 16 de novembro de 2023, a Corte Interamericana de Direitos Humanos (doravante "a Corte Interamericana", "a Corte" ou "o Tribunal") proferiu uma Sentença na qual declarou a responsabilidade internacional da República Federativa do Brasil (doravante "o Estado", "o Estado do Brasil" ou "Brasil") pelo uso desproporcional da força empregada pela Polícia Militar, em 2 de maio de 2000, contra Antônio Tavares Pereira e outros trabalhadores rurais que buscavam manifestar-se publicamente, com a consequente violação de seus direitos à vida, à integridade pessoal, à liberdade de pensamento e de expressão, de reunião, da criança e de circulação. Além disso, o Tribunal considerou o Brasil responsável internacionalmente pela violação dos direitos estabelecidos nos artigos 8.1 e 25.1 da Convenção Americana, em detrimento

> dos familiares do senhor Tavares Pereira e de 69 trabalhadores rurais feridos, devido à falta de devida diligência na investigação e nos processos penais iniciados em razão dos fatos. A Corte também considerou que a longa duração do processo civil, iniciado pelos familiares do senhor Tavares Pereira com o objetivo de obter reparação pelos danos morais e materiais causados, violou a garantia judicial do prazo razoável, prevista no artigo 8.1 da Convenção Americana. Por último, o Tribunal concluiu que o Estado é responsável pela violação do artigo 5.1 da Convenção Americana, devido à violação da integridade pessoal dos familiares do senhor Tavares Pereira, como consequência de sua morte e da subsequente falta de investigação, julgamento e punição dos responsáveis.

Mais uma vez, portanto, o país é condenado pelo descumprimento dos artigos 8.1 e 25.1 da Convenção Americana em razão da ineficácia da persecução criminal, gerando impunidade dos violadores de direitos humanos.

O Caso Honorato e outros também envolveu impunidade de violadores de direitos humanos (Corte Interamericana de Direitos Humanos, 2023a):

> Em 27 de novembro de 2023, a Corte Interamericana de Direitos Humanos (doravante "a Corte Interamericana", "a Corte" ou "o Tribunal") proferiu uma Sentença na qual declarou a responsabilidade internacional da República Federativa do Brasil (doravante "o Estado", "o Estado do Brasil" ou "Brasil") pela execução extrajudicial de 12 pessoas por parte da Polícia Militar, durante a "Operação Castelinho", em 5 de março de 2002. A Corte declarou violados o direito à vida, contido no artigo 4 da Convenção Americana, em detrimento dessas 12 pessoas, e os direitos estabelecidos nos artigos 8.1, 25.1 e 25.2.c) da Convenção Americana, em detrimento de seus familiares, em função da falta de devida diligência e da garantia de prazo razoável na investigação e nos processos penais iniciados, a violação do direito à verdade e a violação do direito ao cumprimento das decisões judiciais em relação às ações civis iniciadas pelos familiares. Por fim, a Corte concluiu que o Estado é responsável pela violação do artigo 5.1 da Convenção Americana, devido à violação da integridade pessoal dos familiares das pessoas executadas, como consequência de sua morte violenta cometida por agentes do Estado e da subsequente falta de investigação, julgamento e sanção dos responsáveis.

Assim, a partir da análise das condenações do Brasil pela Corte Interamericana de Direitos Humanos no tópico acima, identifica-se reiterada violação de obrigações processuais penais positivas decorrente da falta de investigação e punição de delitos contra direitos humanos, gerando cenário de impunidade em solo nacional.

3. IDENTIFICAÇÃO BIOMÉTRICA À DISTÂNCIA EM TEMPO REAL

Estabelecida a natureza jurídica da segurança pública – consistente em atividade estatal a, um só tempo, demandar a atuação ante a ocorrência delitiva e refletir direito fundamental e humano dos indivíduos em exigir a tutela estatal – deflui a relevância dos meios para cumprimento de referido mister, que devem estar em consonância com o tempo atualmente vivido.

Conforme Ferrajoli (2023), a humanidade encontra-se em uma encruzilhada diante de emergências globais que colocam em risco sua própria existência, com destaque para os seguintes fatores: aquecimento global, ameaça de guerra nuclear, aumento da desigualdade, miséria e fome, propagação de regimes despóticos, desenvolvimento do crime organizado e de economias ilegais, e, por fim, o drama de migrantes.

O futuro incerto e aberto requer versatilidade compatível com um mundo em perene modificação (Demercian e Moraes, 2020).

Nesse compasso, o processo de globalização, produtor de externalidades positivas e negativas (Souza e Júnior, 2019), em conjunto com as revoluções tecnológicas e dos costumes, a pós-modernidade e a formação da sociedade de risco colocaram em crise as formas tradicionais de controle social e causaram a necessidade de se repensar o Direito Penal e a política criminal que lhe subsidia, em prol de uma política de segurança pragmática, atenta aos efeitos reais das escolhas tomadas e dos respectivos custos sociais (Moraes, 2016).

Portanto, os desafios impostos pelo presente período, em que há flexibilização de valores, encurtamento do tempo e das distâncias, criminalidade globalizada e mais estruturada, acarretaram o descompasso de conceitos tradicionais do Direito Penal com as atuais formas de criminalidade, a revelar que “a dogmática moderna é ineficiente e excessivamente simbólica sem clara delimitação de suas diversas diretrizes, o que implica leis ineficazes, deslegitimadas socialmente ou sequer conhecidas pelo povo” (Moraes, 2016, p. 231).

O atual momento pode ser denominado de era da robótica, em que os avanços tecnológicos vêm acompanhados da sofisticação criminal e das práticas delitivas, a demandar que o combate à criminalidade também ocorra de forma globalizada, ante atividades ilícitas de índole transnacional (Demercian, 2016).

Surgem, ainda, novos delitos atrelados ao avanço tecnológico e difusão do ciberespaço, os chamados cibercrimes, impulsionados pelo anonimato que impera nas redes (Santos e Araújo, 2023).

Nesse contexto, o processo penal passa a se pautar por "novas expectativas de eficiência, funcionalidade e celeridade" (Demercian, 2016, p. 57).

Impõe-se, então, a fixação de parâmetros para persecução criminal capazes de lidar com os desafios da era atual, que reclama uma política criminal ponderada e proporcional, apta a tutelar a vítima e os bens difusos, consoante lição de Moraes (2016, p. 224):

> Tanto o discurso que se intitula politicamente correto (a prisão não recupera), quanto o discurso que prega tolerância zero (ignorando que grande parcela do aumento da criminalidade está a omissão do Poder Político e das outras esferas de controle social), impedem o bom senso, a racionalidade e uma Política conciliatória que deveriam nortear o tema.
>
> A busca de uma Política Criminal de temperança, moldada pelo bom senso e racionalidade apta a atender as diferentes formas de criminalidade, somente se inicia com o conhecimento desse contexto contemporâneo: o do mundo pós-moderno, pós-industrial e globalizado.
>
> O grande desafio da atualidade é, portanto, constituir a legitimidade de um Direito Penal que pretende tutelar bens transindividuais e, simultaneamente, combater a criminalidade de massa, o terrorismo, as organizações e o crime de colarinho branco, isto é, conciliar modelos eficientes e eficazes de enfrentamento da criminalidade organizada transnacional com os princípios constitucionais do Estado democrático de Direito.

Em síntese, a política criminal racional deve ser "planejada e traçada para uma atuação preventiva menos custosa socialmente e para uma investigação e repressão mais eficientes" (Moraes e Demercian, 2017, p. 27).

A transformação digital, a seu turno, afeta o funcionamento do mundo, que, cada vez mais, depende de operações digitais, que, se, por um lado, permitem inovações a favorecer o bem-estar social, apresentam, por outro, riscos substanciais aos indivíduos e ao próprio desenvolvimento social, na medida em que possibilitam manipulação e concentração do poder sob diversas vertentes (Hoffmann-Riem, 2020).

Há, em tal perspectiva, progressiva conversão da realidade em dados, que podem ser codificados e processados por meio de sistemas de inteligência artificial, fenômeno passível de ser descrito como vigilância de dados (Fontes e outros, 2022). As tecnologias de

reconhecimento facial se desenvolvem, então, nesse contexto de vigilância de dados, impulsionadas pela crescente conversão da realidade em dados processáveis por algoritmos em sistemas de inteligência artificial (Fontes e outros, 2022).

A partir do crescimento do processo de digitalização, com o consequente incremento da utilização de dados, desponta a reflexão sobre a proteção de bens jurídicos relevantes, nomeadamente direitos fundamentais (Hoffmann-Riem, 2020).

Em tal contexto, a emergência dos sistemas de inteligência artificial tem despertado interesse dos operadores e da doutrina especializada em razão tanto da potencialidade de aplicação em diversos campos da segurança pública, com possíveis ganhos à atuação estatal (Zharova, Elin e Panfilov, 2019), quanto dos riscos decorrentes de mencionados sistemas a impor balizas na sua utilização (Gans-Combe, 2022; Gültekin-Várkonyi, 2022).

O uso de inteligência artificial na segurança pública implica benefícios e riscos, havendo controvérsias sobre a forma e a extensão em que a utilização de tal instrumental é pertinente e adequada à consecução de sua finalidade. Para exemplificar essa questão, podem-se citar exemplos da utilização de inteligência artificial para mapeamento da criminalidade, jurimetria com *big data*, policiamento preditivo, avaliação de riscos e reconhecimento facial, todos pontos sobre os quais pairam controvérsias acerca da possibilidade e da extensão de uso da inteligência artificial para tais finalidades.

Sinalizando o benefício da aplicação da inteligência artificial conjugada com a jurimetria, apontam Demercian e Moraes (2020, p. 627):

> É inegável que conciliar a jurimetria com as ferramentas de inteligência artificial disponíveis alterará a forma de funcionamento das instituições do sistema de segurança e de justiça. Demandará novo perfil de profissionais afeitos à criação de modelos preditivos, cruzamento e análise de dados. Quanto mais eficiente é, na era da revolução tecnológica, uma gestão de políticas públicas – tanto na tutela mais eficiente da segurança pública, quanto no trato preventivo de outras políticas públicas cujo déficit também compõe os marcos das causas da criminalidade contemporânea – orientada pela organização dos dados e a sua transformação em informações relevantes. Nesse sentido, a pertinência da jurimetria.

A decisão sobre a forma de utilização da inteligência artificial na segurança pública não é, todavia, meramente técnica, mas depende de ponderação valorativa de acordo com escolhas políticas em cada ordenamento jurídico, em respeito às normativas internas e aos direitos

humanos que incidem sobre a matéria. Sobre a questão, veja-se a lição em estudo sobre a utilização de inteligência artificial na Rússia (Zharova, Elin e Panfilov, 2019, p. 0691, tradução nossa):

> A questão da utilização da inteligência artificial nas esferas judicial e policial não é apenas uma questão de tecnologia e de política da informação, mas é um problema político e parcialmente sócio-psicológico. Como a inteligência artificial faz uma escolha matematicamente baseada em informações estatísticas, é essencial refletir a situação real na informação estatística utilizadas. Ao mesmo tempo, o uso de inteligência artificial pelas agências policiais russas em as suas atividades é dificultado tanto pela falta de prática na aplicação de precedentes como por problemas morais significativos. No entanto, a inteligência artificial pode fornecer assistência significativa no desenvolvimento e criação de locais de trabalho automatizados.

A mera existência de riscos não significa que o uso de inteligência artificial deva ser vedado peremptoriamente para segurança pública, uma vez que tais sistemas não são inerentemente ruins (ou bons), apresentando, por outro lado, potenciais ganhos na efetividade estatal relativamente ao cumprimento do dever de tutela pública. Em tal senda, colaciona-se seguinte excerto sobre a utilização de inteligência artificial no contraterrorismo (McKendrick, 2019, p. 33, tradução nossa):

> Os governos utilizarão novos meios tecnológicos à sua disposição na persecução de objetivos críticos como a segurança pública. O fato de a IA tornar a invasão de privacidade em grande escala muito mais fácil significa que o uso dessas tecnologias continua sendo uma preocupação de política pública. Isso não significa que o uso da IA para prever o terrorismo por democracias liberais deveria estar fora dos limites. Na verdade, boas capacidades preditivas com base na análise automatizada de dados menos intrusivos poderiam fazer parte de restrições sensatas sobre uso desproporcional de medidas que apresentam maiores ameaças à privacidade e outras liberdades. Um processo de tomada de decisão, com desempenho mensurável, sobre quem deve ser os sujeitos a vigilância mais intrusiva pode ser fundamental para limitar o uso de dispositivos tecnicamente habilitados vigilância onde as limitações práticas provavelmente serão eliminadas. Quão bem-sucedidos os estados gerenciam os poderes que a nova tecnologia lhes traz continuará a refletir o quão bem estabelecidas são as suas instituições e a força do seu compromisso com a proteção dos direitos dos cidadãos em geral.

Dentre as temáticas atinentes ao uso de inteligência artificial na segurança pública, talvez uma das que mais tenha despertado controvérsia seja a utilização de tecnologias de

reconhecimento facial (Smith e Miller, 2022), inclusive com situações práticas de repercussão midiática[2].

O tema reclama aprofundamento, na medida em que o reconhecimento facial apresenta diversos desdobramentos, de modo que nem todos os usos são idênticos, a justificar, portanto, que a análise ocorra de forma individualizada a partir do uso pretendido para o sistema.

3.1. TECNOLOGIAS DE RECONHECIMENTO FACIAL E OBJETO DE ESTUDO

Apesar da recente ebulição revolvendo o tema, as tecnologias de reconhecimento facial não são propriamente inéditas.

Em realidade, trata-se de tecnologia estudada há décadas; o recente crescimento do tema, por sua vez, decorre da expansão de sua aplicação por meio de inteligência artificial (Smith e Miller, 2022).

Métodos estatísticos para comparação de rostos foram desenvolvidos na Índia na década de 30, enquanto, em 1964, Woody Wilson Bledsoe, Charles Bisson e Helen Chan Wolf conduziram experimentos em reconhecimento facial no Laboratório de Pesquisa Panoramic, motivo pelo qual as tecnologias de reconhecimento facial não são propriamente novas, nem detêm origem única, mas são "sistemas em movimento" (Taylor, 2024).

Com o surgimento da "Guerra ao Terror" em reação aos ataques terroristas de 11 de setembro de 2001 nos Estados Unidos da América, a tecnologia de reconhecimento facial despertou maior interesse das autoridades em cenário denominado por parte da doutrina de "vigilância algorítmica" (Introna e Wood, 2004), no qual a digitalização de dados permitiu a identificação biométrica automatizada de pessoas por meio de *software* (Introna e Wood, 2004). Em tal panorama, a tecnologia de reconhecimento facial reproduzia vigilância silenciosa, consistente na impossibilidade de o observado interagir com o observador, a realçar sua

---

2 Vide: BARRETO FILHO, H. Polícia usa reconhecimento facial para prender foragidos no meio da folia. **UOL**, São Paulo, 10 fev. 2024. Disponível em: https://noticias.uol.com.br/cotidiano/ultimas-noticias/2024/02/10/reconhecimento-facial-prisoes-foragidos-brasil.htm?cmpid=copiaecola. Acesso em: 28 abr. de 2024; e GRINBERG, F., ARAÚJO, V., FREITAS, H., RIBEIRO, A. Prisões por reconhecimento facial avançam pelo país, mas erros em série desafiam tecnologia de combate ao crime. **O Globo**, Rio de Janeiro e São Paulo, 05 jan. 2024. Disponível em: https://oglobo.globo.com/brasil/noticia/2024/01/05/prisoes-por-reconhecimento-facial-avancam-pelo-pais-mas-erros-em-serie-desafiam-tecnologia-de-combate-ao-crime.ghtml. Acesso em: 28 abr. 2024.

característica velada, de modo a incrementar o interesse das autoridades em tais tecnologias (Introna e Wood, 2004).

Nesse contexto, desenvolveram-se testes para avaliar a precisão dos sistemas, com destaque ao "Facial Recognition Vendor Tests of 2002"[3], realizado por organizações como o Departamento de Estado dos Estados Unidos e o FBI, cuja relevância decorre do tamanho da base de dados utilizada e da atenção a grupos demográficos distintos (Introna e Wood, 2004).

Segundo Introna e Wood (2004), essa primeira edição do teste Vendor teria revelado a falta de precisão das tecnologias de reconhecimento facial, sobretudo ante diferentes grupos demográficos, e a existência de vieses. Citam os autores, inclusive, exemplo de um homem detido no Aeroporto Internacional de Fresno pelo FBI e mandado de volta à origem pelo mero fato de que ele "aparentava ser do Oriente Médio", sem qualquer confirmação de risco concreto ou conduta suspeita. Não por outro motivo os autores teceram contundentes críticas às tecnologias de reconhecimento facial, que, segundo eles, não funcionariam na forma como defendida pelos desenvolvedores e dependeriam de maiores estudos com ênfase em vieses, além de necessitarem de robusta regulamentação legal (Introna e Wood, 2004).

A despeito disso, naquela época, mostrava-se ainda inviável ao sistema, com a tecnologia existente, identificar, automaticamente, indivíduos em meio à multidão, o que era visto como "o grande prêmio" e o projeto mais ambicioso para aplicação dos sistemas de reconhecimento facial (Introna e Nissenbaum, 2010).

As dificuldades existentes na seleção de rostos em situações de baixa qualidade de imagens, luminosidade imprevisível, "ruídos" das imagens de fundo, falta de controle dos cenários, falta de cooperação do sujeito e ângulos das câmeras, tornavam, na época, a identificação remota em tempo real mera aspiração ao futuro, dependente da melhora na tecnologia (Introna e Nissenbaum, 2010).

É com a efervescência da inteligência artificial que o cenário muda, e a tecnologia de reconhecimento facial se torna um dos mais significantes campos de desenvolvimento tecnológico para segurança pública (Smith e Miller, 2022).

Segundo Selwyn *et al.* (2024, p. 13, tradução nossa):

---

3 Ou, atualmente, o primeiro teste Vendor, uma vez que houve edições seguintes (Introna e Nissenbaum, 2010).

> Tal como acontece com todas as formas de IA e tomada de decisão automatizada, o desenvolvimento de TRF (Tecnologias de Reconhecimento Facial) ao longo dos últimos dez anos beneficiou-se de avanços gerais no poder de processamento computacional, especialmente técnicas de aprendizagem profunda e a capacidade de armazenamento de dados necessário para desenvolver e treinar modelos de aprendizado de máquina em grande escala. No entanto, mais especificamente, as formas de TRF que vemos agora na década de 2020 também se beneficiaram dos avanços em hardware de câmera barato e poderoso ao longo da década de 2010 (com câmeras de alta definição instaladas em locais públicos, objetos e dispositivos pessoais), juntamente com a compilação de enormes conjuntos de rostos fotografados, previamente classificados, colhidos de contas de mídia social acessíveis ao público.

O que antes era mera aspiração se tornou realidade com o advento da inteligência artificial, e, hoje, os sistemas de reconhecimento facial são capazes de identificar uma face na multidão, com enorme potencial para resolver crimes (Khan e Rizvi, 2021).

Nesse cenário, o reconhecimento facial não representa uma única tecnologia, mas um termo "guarda-chuva" que engloba um conjunto de tecnologias diversas (Taylor, 2024).

Inclusive, há utilização expansiva no reconhecimento facial para as mais diversas áreas, o que apresentaria potencial para uma função deformadora (*function creep*), como denominado por Selwyn *et al.* (2024), em que mesmo usos legítimos da tecnologia poderiam resultar em abusos.

Logo, atualmente, impulsionadas pela inteligência artificial, as tecnologias de reconhecimento facial passaram a ser desenvolvidas para uma série de finalidades e com diversos propósitos. Incluem-se, por exemplo, as seguintes finalidades: identificação de rostos em fotografias de redes sociais para correspondência com os respectivos perfis, confirmação da identidade de uma pessoa para concessão de acesso a determinados lugares, auxílio para diagnósticos de doenças e para monitoramento de pacientes, avaliação de candidatos em entrevistas de emprego e confirmação de presença em determinados locais (Fontes e Perrone, 2021).

Por conseguinte, o tema não é inequívoco, de modo que a avaliação dos impactos da tecnologia depende de precisa definição do objeto, já que, por exemplo, uma finalidade, como concessão de acesso ao aparelho celular por meio de reconhecimento facial, implica impactos distintos de outra, como avaliação de candidatos em entrevistas de emprego. Os riscos, em tal

toada, são dependentes da forma e da finalidade na qual é utilizada a tecnologia de reconhecimento facial.

Consequentemente, uma conceituação mais precisa das tecnologias de reconhecimento facial, para fins de definição do objeto da presente pesquisa, mostra-se necessária.

Sobre esse aspecto, deve-se, ademais, ter presente a forma de funcionamento da tecnologia de reconhecimento facial.

A identificação humana, em termos científicos, funda-se em cinco pilares, sendo três biológicos e dois técnicos, a saber: unicidade (cada ser é único), imutabilidade (o ser continua o mesmo independente da ação do tempo), perenidade (não desaparece com o envelhecimento), praticabilidade (é passível de ser identificado) e classificabilidade (pode ser alvo de localização quando necessário) (Duarte e outros, 2021).

Os sistemas para identificação de indivíduos, por sua vez, seriam compostos, conforme lição de Introna e Nissenbaum (2010), por três elementos: identificadores atribuídos (aqueles dados ao indivíduo por terceiros, como número de CPF, RG e conta bancária), identificadores biográficos (aqueles decorrentes da história do indivíduo, como endereço, profissão e formação acadêmica) e identificadores biométricos (aqueles relativos a traços físicos do indivíduo, como impressão digital).

Embora tradicionalmente os identificadores atribuídos e biográficos fossem suficientes para identificação da pessoa, incrementou-se, com a aceleração do processo de globalização e a maior mobilidade das populações, a necessidade pela busca de identificadores biométricos para individualização das pessoas, sob a ideia de que “o corpo nunca mente” (Introna e Nissenbaum, 2010).

Assim, as tecnologias de reconhecimento facial (TRF), ou *FRT* (*Facial recognition technology*), sigla pela qual a temática é identificada na literatura estrangeira, se cuida de uma dentre várias tecnologias biométricas destinadas a identificar o indivíduo por meio de suas características pessoais (Hirsoe, 2017).

O termo “biométrica” deriva da língua grega, em que “bio” significa vida e “métrica” se refere à medida de algo (Khan e Rizvi, 2021). Ou seja, a biometria “consiste nas medições de propriedades mensuráveis dos seres vivos e no estudo dessas características em cada indivíduo para verificação automática da identidade” (Duarte e outros, 2021, p. 5).

Nesse contexto, a imagem facial é um tipo de biometria, assim como impressão digital, íris ou DNA, pois contém informação única do indivíduo, de modo a permitir sua identificação e diferenciação em relação aos outros (Lynch, 2024).

As biometrias dividem-se, ainda, em físicas e comportamentais: as primeiras direcionam-se a traços físicos distintivos entre os indivíduos, ao passo que as segundas buscam identificar a pessoa por meio de características de seu comportamento, vide, por exemplo, a cadência de digitação (Khan e Rizvi, 2021).

O reconhecimento facial pode revolver tanto traços físicos como comportamentais dos indivíduos, destacando-se, nesse último ponto, a análise de emoções (Lynch, 2024; Fontes e Perrone, 2021).

Uma das peculiaridades do reconhecimento facial apontada por parte da doutrina consiste na coleta de dados de forma não intrusiva e à distância, diferente da maioria dos outros sistemas de identificação biométrica, cuja coleta de dados depende de formas intrusivas, como, por exemplo, o DNA (Lynch, 2024). Por conta disso, a coleta de dados, no reconhecimento facial, acontece, em boa parte das vezes, sem conhecimento do indivíduo.

A coleta à distância e não intrusiva permite a construção de acervo de imagens dos indivíduos sem o respectivo conhecimento, o que desperta preocupações quanto aos direitos de privacidade, autonomia e correlatos, sobretudo na medida em que a face do indivíduo, por revolver dado biométrico individual, constitui dado sensível[4], passível de especial proteção (Dushi, 2020; Lynch, 2024; Oliveira e outros, 2022).

É exatamente por esse potencial expansivo da tecnologia sem o conhecimento dos indivíduos que emergem, de sua utilização, maiores riscos para as liberdades individuais, com possibilidade para despontar em usos arbitrários (Dushi, 2020; Hirose, 2017).

Em termos específicos de funcionamento, as tecnologias de reconhecimento facial envolvem, em essência, a utilização de técnicas estatísticas para detectar e extrair padrões dos *pixels* da imagem, no intuito de detectar uma face humana e, assim, compará-la com o conteúdo do banco de dados a fim de confirmar uma correspondência (Introna e Nissebaum, 2010).

---

4 Sobre o tema, notar, por exemplo, a definição de dado sensível constante no artigo, 5º, inciso II, da Lei Geral de Proteção de Dados: "dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" (Brasil, 2018b, cap. I, artigo, 5º, inciso II).

Há, em tal contexto, ampla gama de processos automatizados, divididos, grosso modo, nas seguintes etapas: i) captura e detecção da imagem, ii) tratamento da imagem pelos algoritmos de reconhecimento facial, oportunidade em que as imagens são "processadas e transformadas em representações digitais da biometria facial" (Oliveira e outros, 2022, p. 117), criando o *faceprint*, (impressão facial) e iii) comparação do *faceprint* com o constante na base de dados, gerando-se escores de similaridade para definição de uma correspondência positiva ou negativa (Oliveira e outros, 2022).

De modo sucinto, as tecnologias de reconhecimento facial, por meio de processos automatizados e com base em modelos estatísticos, permitem a identificação da face do indivíduo e, dela, extraem os elementos distintivos a formar o chamado *faceprint*, que, por sua vez, é comparado com as imagens existentes no banco de dados para indicar um grau de proximidade a fim de estabelecer eventuais correspondências.

Nessa senda, a tecnologia de reconhecimento facial não fornece resultados definitivos, mas tão somente probabilidades, cuja relevância será determinada a partir das balizas fixadas pelos operadores (*threshold*), conforme demonstra estudo elaborado pela Agência Europeia de Direitos Fundamentais (FRA, 2020).

O *faceprint* identificado pelo sistema gerará um escore de 0 a 100 de similaridade com as imagens constantes no banco de dados, e a identificação positiva ou negativa dependerá da baliza de similaridade (*threshold*) fixada pelos operadores (Oliveira e outros, 2022). Por exemplo, fixando-se o escore de similaridade de 80, as imagens, para serem consideradas uma correspondência (um positivo), deverão ter escore igual ou superior a 80. Abaixando-se a baliza, imagens com menor escore de similaridade serão consideradas como correspondência.

Por isso, existe evidente *trade-off*, na medida em que, quanto mais alta for a baliza estabelecida (isto é, quanto mais similar tiver que ser a imagem para ser considerada um positivo), maior será o número de falsos negativos; por outro lado, quanto menor a baliza, maior o número de falsos positivos (Oliveira e outros, 2022; FRA, 2020).

Estabelecida a forma de funcionamento das tecnologias de reconhecimento facial, adentra-se nas categorias de uso, divididas em três: verificação da identidade de uma pessoa, identificação de uma pessoa e categorização e reconhecimento de emoções (Lynch, 2024).

Na verificação de uma pessoa, existe a comparação denominada "um a um", em que se capta uma imagem para comparação com um único modelo existente no sistema, a fim de confirmar se a pessoa é exatamente aquela cadastrada no sistema (Lynch, 2024; Oliveira e

outros, 2022, FRA, 2020). Conforme a Agência Europeia de Direitos Fundamentais (FRA, 2020, p. 07): “permite a comparação de dois modelos biométricos, geralmente assumidos como pertencentes para o mesmo indivíduo”.

Cuida-se, por exemplo, do uso de tecnologia para acesso ao celular ou a condomínios mediante o reconhecimento da face da pessoa.

Na verificação um a um, a tecnologia não faz julgamentos além do resultado do ato singular de verificação; é dizer, a tecnologia não é capaz de identificar quem estaria buscando acesso além da pessoa previamente autorizada (Selwyn e outros, 2024).

Segundo Lynch (2024), embora exista o risco de fraude e *deep fakes*, essa categoria normalmente é percebida como de baixo impacto para os indivíduos, uma vez que se direciona tão somente à confirmação de identidade singular do indivíduo específico.

A segunda categoria revolve a identificação de uma pessoa no meio de diversas pessoas, em que a comparação não é mais “um a um”, mas “um em muitos” ou mesmo “muitos em muitos” (Lynch, 2024).

Trata-se da situação em que há múltiplas imagens faciais detectadas, podendo ocorrer de forma instantânea – em tempo real – ou de maneira retrospectiva, após a captação da imagem (Lynch, 2024).

Traçando a diferenciação entre verificação e identificação, encontra-se a lição de Akbari (2024, p. 29, tradução nossa):

> O reconhecimento facial que segue a etapa de detecção trata da avaliação da identidade da pessoa na imagem facial extraída e pode ser um processo tanto de identificação quanto de verificação. A identificação facial ocorre quando uma pesquisa 1:N, ou um para muitos, acontece e a imagem do rosto alvo é comparada com um banco de dados de muitas imagens faciais conhecidas. Se a busca for bem-sucedida, a identidade da pessoa na imagem será encontrada. Por exemplo, ao fazer uma verificação policial, uma foto recém-tirada da pessoa pode ser verificada em um banco de dados de fotos criminais para descobrir se essa pessoa tinha algum registro passado. No processo de verificação, ao realizar uma verificação 1:1, ou um para um, estamos na verdade tentando confirmar uma identidade presumida comparando uma nova imagem facial com foto previamente confirmada. Um bom exemplo disso pode ser quando uma foto recém tirada em um posto de fronteira é comparada com a foto no passaporte para confirme que é a mesma pessoa.

A identificação biométrica à distância (comparação de “um em muitos”) é considerada altamente invasiva por envolver a captação de dados sensíveis de diversas pessoas, em geral sem o conhecimento delas (Lynch, 2024). Em razão disso, a doutrina aponta o efeito deletério da tecnologia quanto à liberdade dos indivíduos, com capacidade de redefinir a natureza dos espaços públicos (Oliveira e outros, 2022).

Nessa forma de utilização, a tecnologia de reconhecimento facial pode ser empregada tanto para identificação de uma pessoa precisa, quanto para vigilância em geral, sem alvo determinado (Oliveira e outros, 2022). A primeira estaria ligada à persecução criminal após a ocorrência do crime, enquanto a segunda seria mais direcionada a prevenir a ocorrência de riscos ou o cometimento de crimes (Pereira, 2022).

Existem, ainda, tecnologias que congregam ambas as formas de utilização (identificação e vigilância), permitindo o rastreamento facial (*face tracking*), em que a polícia rastreia suspeitos obtendo informações sobre sua localização e suas atividades (Oliveira e outros, 2022).

É em relação a essa categoria de uso, em que há captação da imagem de diversas pessoas de forma remota e muitas vezes sem o conhecimento delas, que a doutrina expressa maiores preocupações quanto à utilização indiscriminada e com potencial para consequente violação a direitos e liberdades individuais (Dushi, 2020; Lynch, 2024; Oliveira e outros, 2022; Hirose, 2017)

Por fim, a categorização e reconhecimento de emoções compreende a utilização das tecnologias de reconhecimento facial para extração de características das pessoas cuja imagem é avaliada ou para detecção de suas emoções; trata-se de campo experimental e pouco estabelecido, mas que também gera diversas preocupações quanto a impactos em direitos individuais (Lynch, 2024).

Em suma, as tecnologias de reconhecimento facial englobam um conjunto de tecnologias distintas insertas no campo da identificação biométrica, destinadas a identificar/categorizar o indivíduo por meio de suas características faciais. Nesse contexto, gera-se, por meio de processos automatizados e com base em modelos estatísticos, cujos dados são coletados de forma não intrusiva, uma identidade facial (*faceprint*) com os traços distintivos do rosto do indivíduo a ser comparada com as imagens (padrões) existentes no banco de dados e cuja correspondência – positiva ou negativa – será dada a partir de um escore de similaridade, de modo que o sistema não oferece resultados definitivos, mas apenas probabilidades. Dentro desse conceito, existem tecnologias diversas, aplicadas para usos distintos, como verificação da

identidade de uma pessoa singular, identificação de uma pessoa em meio à multidão ou reconhecimento e categorização de emoções, bem como direcionadas para finalidades variadas (concessão de acesso a locais, diagnóstico de doenças, segurança pública etc.), a impor que a análise de impactos aconteça de forma individualizada a partir do uso e da finalidade do sistema.

Isso porque, sendo as categorias de uso e as finalidades variadas, somente mediante análise individualizada é possível identificar os direitos envolvidos e os impactos decorrentes da utilização da tecnologia em específico.

Presente essa conceituação geral sobre as tecnologias de reconhecimento facial, adentra-se mais precisamente no objeto do presente estudo.

No presente trabalho, estuda-se a identificação do indivíduo em meio à multidão para fins de segurança pública.

Cuida-se de reconhecimento facial remoto e em tempo real, exatamente aquele tipo de atividade que desperta grande preocupação da doutrina pelo seu caráter de possível vigilância expansiva e insidiosa, sem o conhecimento dos indivíduos e com possibilidade de alto impacto em direitos e liberdades individuais.

Em tal contexto, o sistema opera à distância e coleta as imagens do indivíduo por meio de câmeras para saber se a pessoa é, em comparação da face captada com o constante no banco de dados, relevante para fins de segurança pública (Pereira, 2022).

A partir do resultado do sistema de identificação biométrica à distância em tempo real, decorre o imediato acionamento das forças de segurança pública, resultando, em regra, na abordagem policial do indivíduo identificado.

Para fins de precisão conceitual, passará a se adotar o termo técnico de referido sistema, que é “sistema de identificação biométrica à distância em tempo real”, conforme constante no Regulamento Europeu. Tendo em vista que, como salientado, a análise do sistema de reconhecimento facial depende da forma de uso e da finalidade do sistema, a precisão semântica é importante para não se cair em confusões sobre o objeto abordado.

Como visto, o sistema de identificação biométrica à distância em tempo real se insere na categoria de identificação de pessoas (comparação de “um em muitos” ou “muitos em muitos”) em tempo real. A tecnologia é não intrusiva quanto à coleta de dados (Lynch, 2024), o que, como salientado, desperta receios atinentes à vigilância velada, própria da vigilância algorítmica (Introna e Wood, 2004).

O tema é polêmico e tem enfrentado acentuada resistência de parcela da doutrina especializada, correlacionando tais mecanismos à emergência de uma sociedade hipervigiada, em um "Estado Big Brother", à semelhança daquele descrito por Orwell (Raposo, 2023; Oliveira e outros, 2022). Defluem diversas preocupações de mencionados sistemas na violação de direitos humanos e fundamentais (FRA, 2020).

A tornar ainda mais espinhosa a temática, a utilização de inteligência artificial, que impulsionou a proliferação de tal tipo de tecnologia, carrega riscos inerentes, a demandar maior cautela ante a autonomia, opacidade e complexidade dos sistemas de inteligência artificial.

A complexidade do tema da inteligência artificial, então, justifica análise específica e pormenorizada.

3.2. INTELIGÊNCIA ARTIFICIAL

A problemática acerca da inteligência artificial inicia na sua própria conceituação, uma vez que não há consenso no ponto, mas pairam diversas abordagens oscilantes entre aspectos mais otimistas ou céticos quanto ao fenômeno (Acypreste e Paraná, 2022).

Por conta disso, Berk (2021) assinala confusão sobre o tema, dependente em como classificar o que é verdadeiramente uma "inteligência artificial". Logo, não haveria uma única conceituação hegemônica, mas diversas definições, todas, todavia, na visão de Berk (2021), com falhas substanciais para englobar o fenômeno como um todo.

Embora fuja do escopo da presente pesquisa esmiuçar as problemáticas em torno da questão, serão brevemente explorados alguns pontos relevantes para conceituação da inteligência artificial a fim de situar o leitor.

Inicialmente, o termo "inteligência artificial" foi apresentado em uma conferência realizada na Universidade de Dartmouth organizada por John McCarthy em 1956, considerado o "pai da IA" (Alzou'bi *et al.*, 2014).

A proposta consistia na ideia de que qualquer aspecto do aprendizado ou outra característica particular da inteligência poderia, em tese, ser detalhadamente descrito ao ponto de uma máquina ser capaz de reproduzir o agir considerado "inteligente", de modo a conseguir resolver problemas que seriam "reservado aos humanos" e, inclusive, em atuação melhor comparativamente ao ser humano (McCarthy e outros, 2006).

Em semelhante linha, encontra-se o Teste de Turing, desenvolvido por Alan Turing na década de 50, no sentido de que uma máquina seria "inteligente" quando desenvolvesse comportamento indiscernível do comportamento humano (Berk, 2021).

Percebe-se que as concepções iniciais de inteligência artificial se fundavam na reprodução (simulação) de comportamento "tipicamente humano" pelas máquinas.

Essa linha de concepção, entretanto, é alvo de críticas, exatamente pelo fato de se preocupar tão somente com o resultado do processamento realizado pela máquina (ou seja, com o *output* gerado) e não pela forma com a qual o processamento é efetivamente realizado (Berk, 2021).

Berk (2021) critica concepções de inteligência artificial que se fundam somente no resultado da atividade desempenhada pelas máquinas, na medida em que haveria mais na inteligência do que o mero processamento de dados.

Para Berk (2021), a inteligência artificial poderia ser dividida em três aplicações distintas: i) inteligência artificial estreita, destinada à realização de tarefas específicas; ii) inteligência artificial geral, capaz de realizar diversas tarefas distintas com base no mesmo conjunto de códigos, como se reunisse diversas inteligências artificiais estreitas; e iii) superinteligência artificial, com potencial de superar a inteligência humana, cuja concretização ainda estaria em um horizonte de, pelo menos, 50 anos. Na época da redação do artigo (em 2020), Berk considerou não haver inteligência artificial geral, apenas inteligência artificial estrita, o que, atualmente, já cai por terra ante a superveniência das chamadas inteligências artificiais de finalidade geral e generativas (vide ChatGPT).

Se, contudo, o mero resultado da atividade não pode definir a inteligência artificial, até porque, atualmente, sabe-se que a capacidade de processamento dos computadores já supera em muito a capacidade humana, remanesce a questão de qual aspecto definiria o conceito de inteligência artificial.

Aqui desponta relevância outra compreensão do fenômeno, que não foca no resultado da atividade, mas na forma pela qual ela é realizada pela máquina, ponto bem explicado por Goodfellow *et al.* (2016, p. 1, tradução nossa):

> Nos primórdios da inteligência artificial, o campo rapidamente abordou e resolveu problemas que eram intelectualmente difíceis para os seres humanos, mas relativamente simples para os computadores – problemas que podem ser descritos por uma lista de regras matemáticas formais. O verdadeiro desafio à

> inteligência artificial provou ser resolver tarefas que são fáceis de serem executadas pelas pessoas, mas difíceis de serem descritas formalmente – problemas que resolvemos intuitivamente, que parecem automáticos, como reconhecer palavras faladas ou rostos em imagens.

Seriam, portanto, os problemas intuitivos que realmente representariam o verdadeiro desafio da inteligência artificial e o seu diferencial em relação a outras tecnologias.

Nessa senda, no intuito de diferenciar a inteligência artificial (IA) das tradicionais tecnologias da informação (TI), Akbari (2024) traça os seguintes pontos: instruções, código e manutenção.

Enquanto as tecnologias da informação tradicionais dependem de instruções explícitas e passo-a-passo, contidas em seu código, com necessidade de manutenção periódica para reparação de erros (*bugs*) e melhoria de seus componentes, a inteligência artificial recebe objetivos que são trabalhados pelo próprio sistema para encontrar a melhor solução, de modo que os códigos são baseados em conhecimento (*knowledge base*) a fim de permitir encontrar o melhor resultado (*output*) para as informações recebidas (*inputs*), sendo que o sistema não depende de manutenção periódica, mas reclama monitoramento contínuo para prosseguir no desempenho adequado à sua finalidade durante seu "ciclo de vida" (Akbari, 2024).

Segundo Akbari (2024, p. 30, tradução nossa), uma das melhores definições para inteligência artificial seria aquela desenvolvida pela OCDE (Organização para a Cooperação e Desenvolvimento Econômico), no sentido de que:

> A Inteligência Artificial (IA) refere-se a sistemas de computador que podem executar tarefas ou fazer previsões, recomendações ou decisões que geralmente requerem inteligência humana. Os sistemas de IA podem executar essas tarefas e tomar essas decisões com base em objetivos definidos por seres humanos, mas sem instruções.

Perceba-se que a característica singular seria a falta de instruções a revelar autonomia da máquina para alcançar o objetivo proposto pelo desenvolvedor.

Para fins do presente trabalho, parte-se, primeiramente, da concepção de inteligência artificial constante no artigo 3º do Regulamento Europeu (até porque se trata do marco legislativo aqui aprofundado), que considera sistema de inteligência artificial como (União Europeia, 2024, p. 46):

> [...] um sistema baseado em máquinas concebido para funcionar com níveis de autonomia variáveis, e que pode apresentar capacidade de adaptação após a implantação e que, para objetivos explícitos ou implícitos, e com base nos dados de entrada que recebe, infere a forma de gerar resultados, tais como previsões, conteúdos, recomendações ou decisões que podem influenciar ambientes físicos ou virtuais.

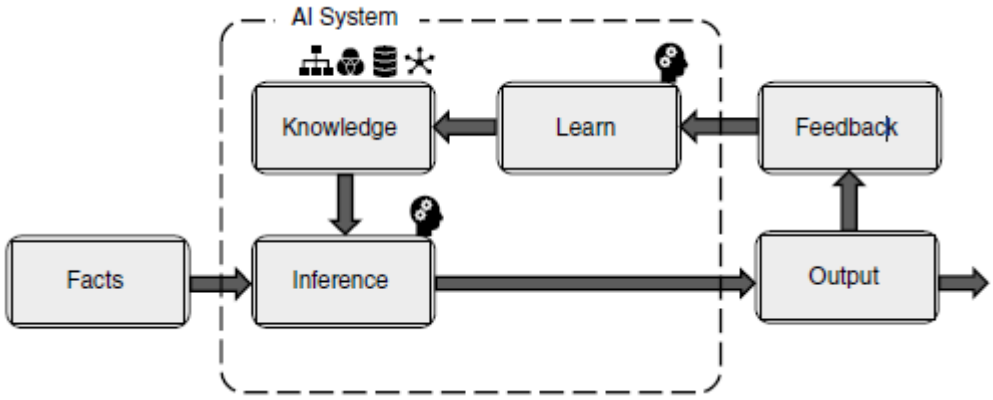
Por essa concepção, verifica-se que o traço distintivo do sistema de inteligência artificial seria a capacidade de inferência com base em máquinas, o que, segundo Madiega (2024), encontra-se de acordo com a literatura especializada sobre o tema e ostenta abrangência para abarcar modelos mais elaborados de inteligência artificial, como as inteligências artificiais de finalidade geral ou generativas, surgidas no curso da elaboração do Regulamento Europeu.

Entende-se que a concepção do Regulamento Europeu é adequada, na medida em que destaca o ponto principal dos sistemas de inteligência artificial atualmente: a capacidade de inferência baseada em máquinas, de modo que o sistema opera com autonomia ante os objetivos fixados pelo operador.

Nada obstante, há mais um ponto relevante para funcionamento do sistema de inteligência artificial, qual seja, a capacidade de aprendizado (Akbari, 2024).

O sistema de inteligência artificial, ao receber os fatos (*inputs*), realiza inferências a partir da base de conhecimento a ele passada (*knowledge base*), gerando os resultados (*outputs*), que, por sua vez, são alvo de retorno (*feedback*) pelo ambiente, no sentido de indicar se os resultados se mostraram adequados ou não aos objetivos fixados (Akbari, 2024). Com base nesse retorno, *feedback*, a máquina aprende e vai aprimorando sua base de conhecimento, conforme ilustra a figura abaixo (Akbari, 2024):

Figura 1 – Elementos chaves do sistema de inteligência artificial



Fonte: Extraído de Akbari (2024, p. 35).

As formas de aprendizado da máquina podem variar caso haja supervisão humana ou não.

Enquanto as inteligências artificiais tradicionais (ou GOFAI – *good and old fashioned artificial intelligence*), descritas como inteligências artificiais simbólicas, dependem da interferência humana no processo de aprendizagem, os sistemas baseados em aprendizado pela própria máquina (*machine learning*) realizam de forma automatizada o processo de aprendizagem a partir dos dados obtidos (Akbari, 2024). Por conta disso, ante a falta de participação humana no processo, os resultados do aprendizado pela própria máquina são uma "caixa-preta" (*black box*) e pouco previsíveis (Akbari, 2024).

Nesse contexto de aprendizado pela máquina, destacam-se as redes neurais profundas (ou *deep neural networks*), em que as técnicas de aprendizado pela máquina são conjugadas com estruturais de redes neurais, a possibilitar maior aprofundamento no processo de aprendizagem (Akbari, 2024).

Exatamente por isso a seleção de dados e o treinamento do sistema com dados de qualidade são essenciais ao desempenho dos sistemas de inteligência artificial (Akbari, 2024). Quanto maior a quantidade de dados, maior será a precisão dos sistemas de inteligência artificial (Burrell, 2016).

Para fins de conceito do presente trabalho, define-se o sistema de inteligência artificial pela capacidade de inferência baseada em máquinas, destinada à solução autônoma de problemas diante de objetivos fixados pelo operador e a partir de uma base de conhecimento estabelecida, com potencial para aprender em função dos resultados gerados, aprimorando continuamente o seu desempenho na finalidade pretendida.

Feita essa conceituação, cumpre averiguar quais desafios são impostos por essa capacidade de inferência e autonomia das máquinas na realização de tarefas fixadas pelo ser humano, sobretudo quando tais tarefas dizem respeito à segurança pública.

Como bem colocam Fiordi *et al.* (2018, p. 689, tradução nossa), a inteligência artificial "é uma força poderosa, uma nova forma de agência, que já está redesenhando nossas vidas, nossas interações e nosso ambiente".

Por conseguinte, o debate não se insere mais na possibilidade de impacto da inteligência artificial em nossa sociedade, uma vez que isso já se trata de uma realidade, mas, sim, em qual medida esse impacto será positivo ou negativo e para quem (Fiordi e outros, 2018).

Em síntese, com a inteligência artificial, vêm diversas oportunidades, bem como riscos (Fiordi e outros, 2018).

Presente que a inteligência artificial é capaz de processo de inferência atrelado ao processamento de dados em potencial muito superior à mente humana, percebem-se enormes potenciais de inovação que tais tecnologias trazem. A capacidade de inovação da inteligência artificial é bem descrita pelo item 4 do preâmbulo do Regulamento Europeu (União Europeia, 2024, p. 2):

> A IA é uma família de tecnologias em rápida evolução que contribui para um vasto conjunto de benefícios económicos, ambientais e sociais em todo o leque de indústrias e atividades sociais. Ao melhorar as previsões, otimizar as operações e a repartição de recursos e personalizar as soluções digitais disponibilizadas às pessoas e às organizações, a utilização da IA pode conferir importantes vantagens competitivas às empresas e contribuir para progressos sociais e ambientais [...].

Ao analisar os potenciais econômicos da inteligência artificial, a OCDE assentou sua capacidade para diminuir custos e permitir melhores decisões, gerando ganhos de produtividades, melhorando o bem-estar e auxiliando na resolução de desafios complexos (OCDE , 2019).

Pelo fato de os sistemas de inteligência artificial serem capazes de oferecer enormes benefícios sociais, a postura de Autoridades Públicas perante o assunto tende a ser geralmente positiva (Winfield e Jirotka, 2018).

Apesar disso, os potenciais ganhos da inteligência artificial vêm atrelados a riscos inerentes a tais sistemas (Winfield e Jirotka, 2018).

Isso porque a inteligência artificial, ao operar mediante inferências realizadas por máquinas a partir do processamento de larga quantidade de dados, muito além da capacidade humana, apresenta opacidade e complexidade (Madiega, 2024; Burrell, 2016).

Os sistemas são complexos, uma vez que a capacidade de processamento é muito superior à racionalidade humana, e opacos, na medida em que não há como rastrear precisamente os motivos do resultado obtido pela máquina, exatamente por se tratar de uma inferência e não do resultado da observância de um código estrito (Madiega, 2024; Burrell, 2016)[5].

Assim, os sistemas de inteligência artificial exibem comportamento autônomo e imprevisível, que vai, ao longo do tempo, alterando-se; ademais, exatamente por esse aspecto de aprendizagem, o sistema depende de dados de qualidade para funcionar adequadamente (Madiega, 2024).

Inexiste, aliás, profundidade semântica própria dos sistemas de inteligência artificial, pois estes dependem dos dados que lhe são passados, tornando-os passíveis de erros crassos (Pasquinelli, 2019). São sistemas, então, cuja precisão é estritamente relacionada com os dados que lhe são alimentados (Burrell, 2016).

Nesse contexto, defluem os riscos de tais sistemas, uma vez que a complexidade, a opacidade e a autonomia geram comportamentos imprevisíveis, com resultado potencialmente não esperado, além do fato de que a dependência de dados de qualidade para operar de forma adequada impõe a necessidade de controle e treinamento contínuos dos sistemas.

São, portanto, sistemas que carregam consigo perigos inerentes

5 Sobre o ponto, é pertinente assinalar que Burrell (2016, p. 2, tradução nossa) aponta a existência de três tipos de opacidade: 1) opacidade decorrente da intenção corporativa de proteger o conhecimento sobre o funcionamento da máquina; 2) opacidade pela falta de conhecimento na leitura de códigos que recai sobre poucos especialistas; e 3) opacidade decorrente da "incompatibilidade entre a otimização matemática em alta dimensionalidade característica do aprendizado de máquina e as demandas de raciocínio e estilos de interpretação semântica próprias da escala humana". Esse último tipo decorre das técnicas de aprendizado pela máquina (Burrell, 2016) que seria a verdadeira opacidade, uma vez que a forma de processamento das máquinas para alcançar as inferências, baseadas em modelos matemáticos e algoritmos, seriam incompreensíveis à forma de raciocínio humano.

Sobre os riscos, é interessante rememorar a lição de Ulrich Beck (1992, p. 21), no sentido de que o "risco pode ser definido como uma forma sistemática de se lidar com os perigos e as inseguranças induzidas e introduzidas pela própria modernização".

O risco se relaciona com a força da modernização e a consequente globalização da dúvida, em que a administração do risco decorre de decisões políticas, sendo, por isso, politicamente reflexiva (Beck, 1992).

Os riscos refletem decisões políticas de como enfrentar perigos e inseguranças contemporâneos. Contextualizando ao caso, o fato de os sistemas de inteligência artificial apresentarem perigos e incertezas não seria suficiente para barrar o seu uso, diante dos potenciais inovadores que trazem, razão pela qual a solução ocorre pela via política mediante administração do risco.

Em suma, o potencial inovador dos sistemas vem atrelado a riscos a serem ponderados politicamente, conforme bem descrito pelo item 5º do preâmbulo do Regulamento Europeu (União Europeia, 2024, p. 2):

> Ao mesmo tempo, em função das circunstâncias relativas à sua aplicação, utilização e nível de evolução tecnológica específicos, a IA pode criar riscos e prejudicar interesses públicos e direitos fundamentais protegidos pela legislação da União. Esses prejuízos podem ser materiais ou imateriais, incluindo danos físicos, psicológicos, sociais ou económicos.

Quanto à segurança pública, os sistemas de inteligência artificial trazem arcabouço técnico a auxiliar o Estado no cumprimento das obrigações processuais penais positivas, sem, todavia, deixar de ensejar riscos inerentes, até mais acentuados, em razão da importância dos bens jurídicos tutelados pela esfera penal e seu caráter de *ultima ratio* ante a potencialidade de constrição de liberdade do investigado.

Sobre os pontos positivos, Zharova, Elin e Panfilov (2019) trazem diversos campos em que a inteligência artificial pode auxiliar a segurança pública, como em análises criminais, investigativas e estratégicas, além de auxiliar o operador na condução de procedimentos e processos decisórios complexos, com redução ao tempo de consulta de documentos e diminuindo risco de erros e imprecisões.

Também há menções positivas ao mapeamento delitivo (Pádula e outros, 2016). Berk (2021), por sua vez, sustenta que os sistemas de inteligência artificial trazem mais segurança jurídica e objetividade ao sistema de justiça criminal, de modo a representar *trade-off* positivo em comparação às alternativas.

Em geral, as novas possibilidades oriundas da utilização de sistemas de inteligência artificial auxiliam processos complexos de tomada de decisão e influenciam políticas em direção ao aprimoramento da administração e atuação nos domínios públicos (Fontes e outros, 2022).

Inclusive, especificamente ao uso de tecnologia de reconhecimento facial, Rola (2022) aponta se tratar de uma inevitabilidade social e tecnológica, já sendo realidade em diversos países, tecendo as seguintes considerações (Rola, 2022, p. 80-81):

> A IA congrega a facilidade e a agilidade em extrair e agregar metadados de imagens digitais, sobre homens, mulheres, crianças, veículos, objetos, tamanho, cor, velocidade, caminho, antecedentes e, muito mais, em formatos quantitativos, qualitativos, de abeiramento, de separação isolada, comparativa, abrindo novos horizontes de investigação criminal, na ordem pública, como auxílio a decisão estratégica dos profissionais de segurança pública.
>
> [...]
>
> Graças às tecnologias de mobilidade digital, conjugadas com os processamentos de imagens digitais, podem contribuir para a realização dos objetivos de prevenção criminal, ou seja, reduzir o número de ilícitos criminais, evitar a prática sistemática de crimes e, assim, contribuir para a luta no aumento da segurança. As imagens processadas por IA podem fornecer informações aos operacionais presentes no terreno e, portanto, contribuir para incrementar na SP uma política mais proativa e menos reativa.

Sobre a tecnologia, Oliveira *et al.* (2022) citam exemplo da ONG americana Thorn, que, mediante emprego de reconhecimento facial, teria conseguido resgatar mais de 10 mil crianças vítimas de tráfico sexual.

Em semelhante toada, a polícia da Índia indiciou que, em 2018, o uso de tecnologia de reconhecimento facial permitiu a identificação de 3000 crianças desaparecidas em somente 4 dias (Zalnieriute, 2024).

Khan e Rizvi (2021), por sua vez, destacam a alta capacidade da tecnologia de reconhecimento facial para resolver crimes, com potencial de "revolucionar todo o sistema de justiça criminal", sem deixar de pontuar, por outro lado, substanciais questões éticas e de privacidade que emergem da questão. Como salientado, o potencial inovador não deixa de vir atrelado a riscos.

Esses riscos, na seara da segurança pública, são realçados ante a possibilidade de arbitrariedade estatal, invasão de privacidade e discriminação contra grupos minoritários.

Em estudo sobre as oportunidades e os riscos da inteligência artificial, Raso *et al.* (2018) assinalam os seguintes impactos negativos em direitos humanos pela utilização de inteligência artificial na justiça criminal: direito a uma audiência pública justa, presunção de inocência e direito à privacidade.

Para chegar a tais conclusões, os autores apontam que a complexidade e opacidade dos sistemas de inteligência artificial dificultam a sua impugnação perante o Poder Judiciário, violando os direitos a um julgamento justo e à presunção de inocência (Raso e outros, 2018). Ademais, os sistemas dependeriam de grande quantidade de dados pessoais e sensíveis, trazendo grandes preocupações relativas ao direito de privacidade dos indivíduos (Raso e outros, 2018).

Não por outro motivo, então, a maior parte da doutrina examina com restrições (por vezes severas) a aplicação dos sistemas de inteligência artificial para fins de política criminal e segurança pública.

Por exemplo, sobre o mapeamento da criminalidade, Brayne (2022) aponta seu potencial a incrementar padrões discriminatórios, por aumentar policiamento e atuação da polícia em áreas marginalizadas, alimentando o algoritmo com tais dados, a gerar o que a autora chama de uma profecia "auto-realizável".

Já especificamente sobre a utilização do reconhecimento facial por inteligência artificial, Costa e Kremer (2022) apontam tendência internacional ao banimento, devido aos potenciais vieses discriminatórios contra grupos vulneráveis. Afirmam os autores que o reconhecimento facial por inteligência artificial (Costa e Kremer, 2022, p. 162):

> [...] tem sido uma ferramenta de reprodução e potencialização de opressões já existentes na sociedade, pois, ao delegar aos algoritmos a tarefa de identificar e apontar suspeitos, confere-se à seletividade penal uma aparência de suposta neutralidade e afastamento da discriminação racial em abordagens policiais.

Embora as questões específicas da identificação biométrica à distância em tempo real sejam esmiuçadas a seguir, adiantaram-se aqui alguns pontos apenas para realçar as controvérsias que, em geral, pairam sobre a utilização de inteligência artificial na segurança pública.

Como visto, as tecnologias de reconhecimento facial, dentro das quais se insere a identificação biométrica à distância em tempo real (objeto do presente estudo), estão nesse contexto do debate sobre a utilização de inteligência artificial na segurança pública, e pontos relevantes para descortinar a temática – como: dependência de dados, treinamento do algoritmo, vieses etc. – decorrem exatamente da natureza da inteligência artificial, motivo pelo qual a abordagem no presente tópico se mostrou fundamental.

Fixadas, então, as particularidades da inteligência artificial, sinalizando-se o seu conceito, forma de funcionamento, riscos e potencial de inovação, traçando o paralelo com as tecnologias de reconhecimento facial, cumpre adentrar propriamente no objeto do presente estudo, qual seja, a identificação biométrica à distância em tempo real para fins de segurança pública.

3.3. FASES DE IMPLEMENTAÇÃO DO SISTEMA

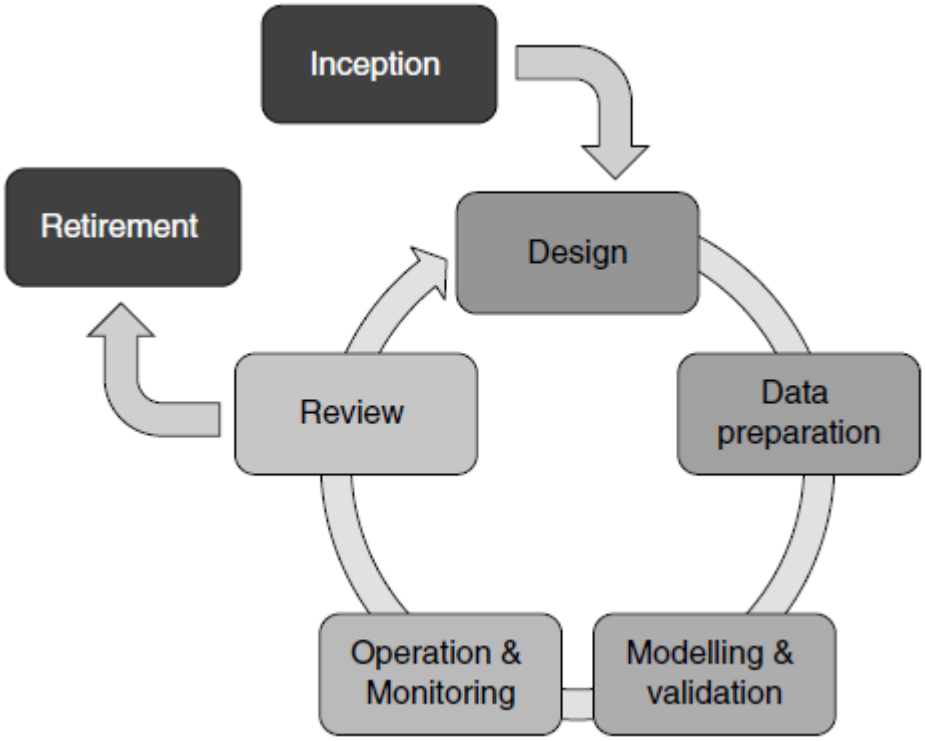
Como visto, a identificação biométrica à distância em tempo real – anteriormente considerada o projeto mais ambicioso para aplicação dos sistemas de reconhecimento facial (Introna e Nissenbaum, 2010) – é possível em razão da utilização de inteligência artificial.

Consequentemente, as características inerentes a sistemas de inteligência artificial também serão reproduzidas na implantação de tecnologias de identificação biométrica em tempo real.

Afora a introdução feita à inteligência artificial, notadamente ao processo de aprendizado pela máquina (*machine learning*), é relevante abordar as etapas de implementação do sistema, com relevância para a identificação biométrica à distância em tempo real.

Sobre o tema, Akbari (2024) identifica cinco estágios relevantes no ciclo de vida da inteligência artificial, a saber, desenho (*design*), preparação de dados (*data preparation*), modelamento e validação (*modelling & validation*), operação e monitoramento (*operation & monitoring*) e revisão (*review*), conforme ilustra a figura abaixo:

Figura 2 – Ciclo de vida de um sistema de inteligência artificial



Fonte: Extraído de Akbari (2024, p. 32).

Referida figura demonstra, inclusive, que os processos acontecem de forma contínua, é dizer: durante o ciclo de vida da inteligência artificial, os resultados da revisão do sistema podem justificar alterações no desenho a ensejar nova preparação de dados e novos modelos a serem validados, de modo que o projeto inicial é um contínuo e não uma solução pronta e hermética.

A partir da concepção de uma ideia ou da identificação de uma necessidade, constrói-se o desenho da inteligência artificial, etapa em que muitas decisões críticas são tomadas, baseadas

em hipóteses e que poderão ser corrigidas em etapas seguintes; tais decisões englobam, dentre outros, os dados a serem coletados, expectativas quanto às características dos dados, disponibilidade para treinamento de dados ou oportunidades para criá-los, algoritmos compatíveis, critério de aceitação antes de entrar em uso (Akbari, 2024).

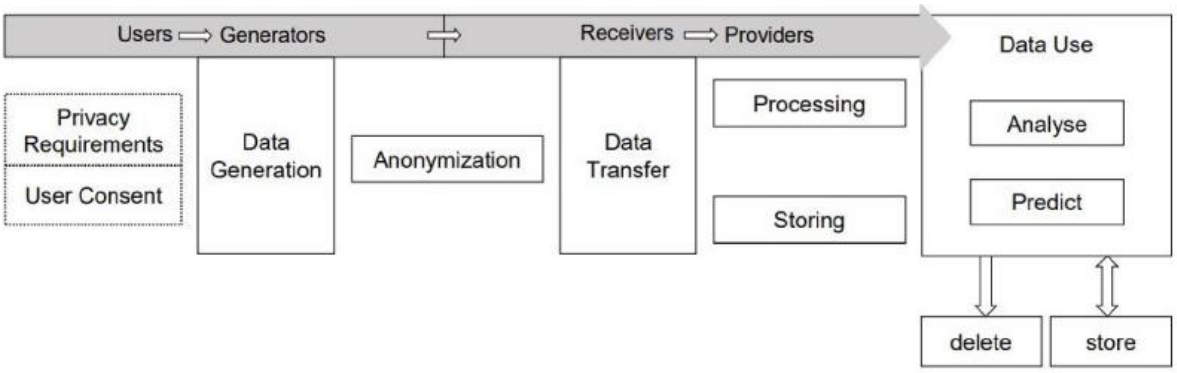
Nessa fase, os propósitos do sistema são relevantes para definição de seu desenho, na medida em que as formas de coleta dos dados e o ambiente em que será utilizada a tecnologia de reconhecimento facial impactam o desenho; por exemplo, sistemas feitos para operar em ambiente interno e controlado incorrerá em desempenho fraco em condições diversas, como em ambiente externo e caótico (Akbari, 2024).

A preparação de dados, por sua vez, pode ser um dos momentos a mais consumir tempo e um passo crítico da implementação da inteligência artificial (Akbari, 2024).

Nesse estágio, cobrem-se os seguintes pontos: coleta de dados, verificação de sua qualidade, recursos de engenharia e categorização (Akbari, 2024).

Segundo Fontes *et al.* (2022), a dependência de dados é uma característica inerente da inteligência artificial, que a permite adquirir funcionalidade. Os autores, todavia, apontam que o ciclo de vida dos dados e da inteligência artificial não apresentam a mesma linha temporal, com o seguinte exemplo para o tratamento de dados (Fontes *et al.*, 2022):

Figura 3 – Exemplo do ciclo de vida dos dados



Fonte: Extraído de Fontes *et al.* (2022, p. 06).

Como se percebe, a extração e a análise de dados seguem dinâmica própria, com peculiaridades associadas ao direito dos titulares dos dados, notadamente o direito à privacidade, do qual emerge a questão do consenso (Fontes *et al.*, 2022).

Em termos de identificação biométrica em tempo real, a discussão sobre o consenso se torna ainda mais complicada, uma vez que há uma situação paradoxal em que transparência e eficiência parecem não se compatibilizar para o uso da tecnologia (Fontes *et al.*, 2022). Na análise da questão, Fontes e Perrone (2021) apontam que a perda da privacidade em razão da implementação de sistemas de reconhecimento facial poderia se justificar como um compromisso assumido pela sociedade para evitar males sociais, como a ocorrência de crimes.

Verifica-se, então, que a própria coleta e tratamento de dados já se interliga com questões jurídicas relacionadas à autonomia e à privacidade dos indivíduos, pois não apenas o rosto se trata de dado sensível, como, tratando-se de sistema direcionado à execução de política de segurança pública, sua eficiência, ao eventualmente se condicionar ao consenso da pessoa visada, ficaria prejudicada.

Além disso, deve-se ter em mente que o aumento de dados de qualidade, ao mesmo tempo em que produz sistemas mais robustos, torna mais custosa a gestão de referidos dados (Akbari, 2024).

Inclusive, na identificação biométrica à distância, a qualidade dos dados é fundamental, na medida em que, para possibilitar a comparação com maior chance de êxito, há requisitos absolutos (desobstrução da face, resolução e nitidez) e relativos das imagens de referência (Duarte *et al.*, 2021).

Uma vez preparados os dados do sistema, começa-se o seu desenvolvimento, estágio em que serão buscados os algoritmos mais adequados e as configurações mais pertinentes, com treinamento de modelos e validação a fim de definir a adequação aos objetivos propostos (Akbari, 2024). Aqui, definem-se as balizas de níveis de aceitação para os escores de similaridade considerando o balanço entre falsos positivos e falsos positivos, além de se checar vieses entre populações demográficas distintas, notadamente em razão de gênero e etnia (Akbari, 2024).

Ao finalizar o processo de modelamento e validação, segue-se para operação e monitoramento, oportunidade em que o funcionamento do sistema de inteligência artificial deve ser supervisionado ante a possibilidade de alteração do desempenho ao longo do tempo, a reclamar monitoramento constante (Akbari, 2024).

Por fim, a revisão pode acontecer de forma periódica ou com base em gatilhos específicos, levando a avaliação sobre eventual necessidade de alteração do desenho da inteligência artificial para lidar com novas circunstâncias que despontaram em razão de seu uso (Akbari, 2024).

Assentada a forma de desenvolvimento da inteligência artificial que dará suporte ao sistema de identificação biométrica, cumpre averiguar os métodos por meio do qual a identificação biométrica se concretiza.

Akbari (2024) aponta que os métodos antigos para detecção facial seriam baseados na extração de características faciais convertidas em vetores numéricos, com regras pré-definidas de como identificar uma face, a tornar o reconhecimento facial um problema de regressão.

Esse método, mais simples e limitado, resulta em processo mais transparente e explicável, mas com baixo desempenho caso as condições das imagens diminuam (Akbari, 2024).

Superando o método de análise de características faciais, há as abordagens holísticas, popularizadas após a introdução do chamado *Eigenfaces* na década de 90 pelos pesquisadores Turk e Pentland; em vez de detectar características da face baseadas em uma definição facial, essa abordagem considera a imagem com suas formas de *pixel* para formar vetores em espaço dimensional e aplicar técnicas de redução combinadas com abordagens matemáticas e estatísticas que não se fiam somente no que está na imagem em si (Akbari, 2024).

Em tal método, vigoram técnicas de aprendizado de máquina (*machine learning*) em relação aos dados colhidos, sofrendo, todavia, com desafios de suposições baseadas em distribuição estatística, que podem piorar a análise da imagem controlada (Akbari, 2024).

Por fim, as redes neurais profundas (*Deep neural networks*) representaram avanço e sucesso no campo do reconhecimento facial, ao permitir maior desenvolvimento das abordagens holísticas (Akbari, 2024).

Atualmente, a identificação biométrica à distância em tempo real se desenvolve a partir de sistemas de inteligência artificial calcados no processo de aprendizagem pela máquina, notadamente por meio de redes neurais profundas.

Sumarizando-se as etapas da identificação facial, é possível descrever os seguintes passos (Oliveira *et al.*, 2022, p. 117):

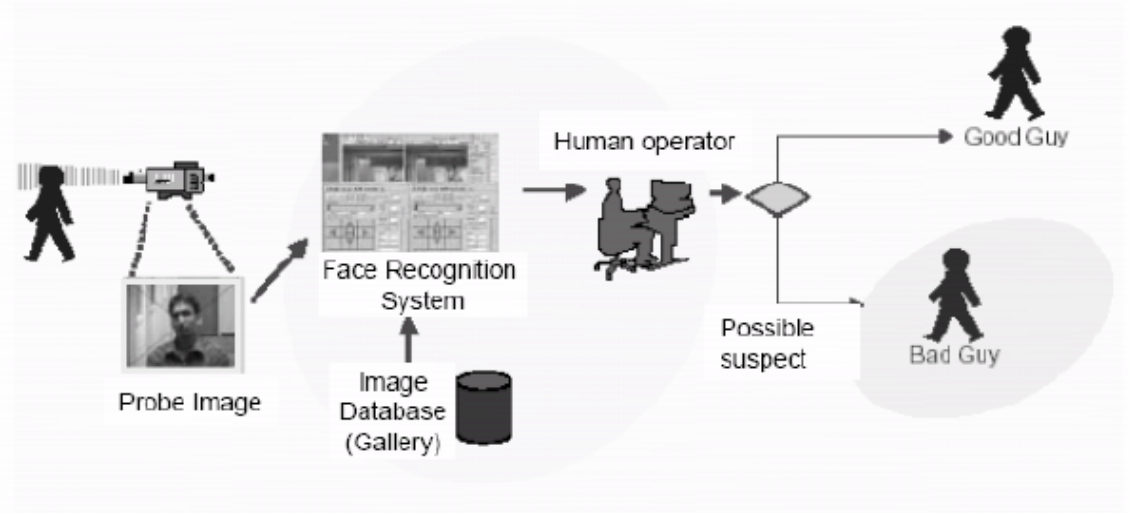
> O processo de reconhecimento facial pode ser dividido em etapas (BUOLAMWINI *et al*, 2020). A captura e detecção relaciona-se com a obtenção da imagem ou fotografia. A circunstância de captura pode ser: para verificação de identidade para acesso a dispositivo ou serviço; em ambientes controlados; de forma voluntária ou não; e ainda a coleta de imagens disponíveis em redes sociais. Já a inscrição, tradução livre de *enrollment*, é o processo de coleta de informação visual de um indivíduo para formação de uma galeria ou banco de dados (BUOLAMWINI*et al*, 2020).
>
> Em seguida, os dados colhidos em etapas anteriores são tratados por algoritmos de reconhecimento facial. Tradicionalmente, algoritmos de reconhecimento podem ser divididos em abordagens geométricas relativas a características fotométricas ou distintivas, permitindo uma classificação entre algoritmos holísticos – aqueles que buscam reconhecer completamente a face –e os métodos *feature-based* – aqueles que analisam características faciais locais (como olhos, nariz e boca) e armazenam parâmetros e métricas como ângulos e distâncias entre os pontos fiduciais no rosto como descritores para comparação futura no processo de reconhecimento facial (GALTERIO *et al*, 2018; JOSHI; GUPTA, 2016; PETRESCU, 2019).
>
> Assim, nesta etapa, as imagens são processadas e transformadas em representações digitais da biometria facial, sendo o objetivo a criação de representações digitais dos rostos presentes nas imagens. Tais representações são chamadas de *faceprints*. Os *faceprints* devem ser desenvolvidos de forma a alcançara maior acurácia possível para a próxima etapa, que consiste em comparar duas imagens da mesma pessoa (BUOLAMWINI *et al*, 2020). Em um processo de identificação, a etapa de comparação envolve identificar um *faceprint* e compará-lo a outros disponíveis na base de dados/galeria, gerando escores de similaridade, computados para estimar o quão parecidos são dois *faceprints* (BUOLAMWINI *et al*, 2020).
>
> A decisão sobre a correspondência nas TRFs de identificação são as mais relevantes para aplicações em segurança pública, nosso foco no presente artigo. Na obtenção de resultados quanto a correspondência, os processos resultantes de TRFs de identificação indicam vários rostos no banco de dados/galeria que potencialmente correspondem ao rosto submetido (BUOLAMWINI *et al*, 2020). Nos referiremos à lista de resultados como a relação de candidatos à correspondência correta. No Quadro 1 sintetizamos as possíveis respostas à etapa de correspondência.

Cuida-se do processo já descrito anteriormente no subtópico 3.1.

Relativamente à identificação biométrica à distância em tempo real, a câmera vai captar a imagem facial da pessoa e confortá-la com o constante no banco de dados para, mediante o escore de similaridade, definir a ocorrência de uma correspondência positiva.

A situação é ilustrada, grosso modo, pela figura abaixo:

Figura 4 – Visão Geral de um Sistema de Reconhecimento Facial



Fonte: Extraído de Introna e Nissenbaum (2010, p. 11).

A figura revela a participação do operador humano no processo, após a indicação de correspondência pelo sistema de reconhecimento facial.

Embora os processos de reconhecimento facial sejam cada vez mais automatizados (Akbari, 2024), mostra-se importante a participação humana exatamente para evitar a incorrência da máquina em erros crassos (Pasquinelli, 2019). Aliás, a supervisão humana se trata de um princípio adotado no âmbito do próprio Regulamento Europeu da Inteligência Artificial, o que reforça que o resultado da identificação biométrica deve passar pelo crivo de um ser humano, de modo a não gerar ações de forma instantânea e imediata.

Por fim, um último tópico relevante à implementação do sistema diz respeito à localização das câmeras, que serão o *hardware* a obter as imagens dos suspeitos.

O ponto é relevante, na medida em que já se apontou, quanto a projeto implementado na cidade de Detroit (Estados Unidos da América), que as câmeras para fins de vigilância foram colocadas primordialmente em áreas habitadas pela população negra, o que representaria falta de equidade e agravamento de discriminações (Najibi, 2020).

Assim, além das questões relativas ao desenvolvimento da tecnologia em si, o local de colocação das câmeras é ponto relevante, sobretudo para se evitar vieses discriminatórios a acentuar desigualdades sociais.

Em suma, percebe-se que a implementação de sistemas de identificação biométrica à distância em tempo real seguirá os passos do ciclo de vida da inteligência artificial, pois dependentes de tal tecnologia.

Deverá ser objeto de desenho, preparação de dados, modelamento e validação, operação e monitoramento, e revisão, de forma contínua, para garantir o desempenho adequado de suas funções. Nesse contexto, a dependência de dados é uma característica importante e que desperta questões cruciais, uma vez que os dados biométricos são sensíveis e passíveis de proteção especial, necessitando-se, portanto, de maiores cuidados no momento da coleta.

O funcionamento da inteligência artificial, por sua vez, se funda em abordagens holísticas (por vezes combinadas com método de análise de características faciais) em processo de aprendizagem pela máquina, notadamente por meio de redes neurais profundas, o que salienta a dependência de dados e de adequado treinamento do algoritmo. Além disso, é importante que o resultado do sistema passe por supervisão humana, não gerando ações automáticas. Um último ponto reflete a questão relativa às localizações das câmeras, que, se focarem apenas em áreas marginalizadas, podem servir para incrementar desigualdades, com risco de maiores vieses em abordagens.

A implementação do sistema de identificação biométrica à distância em tempo real passa por esses estágios, que, como se percebe, revelam a complexidade do tema, na medida em que há diversas etapas interligadas e que a falha em uma delas é capaz de prejudicar o desempenho do sistema como um todo.

Feito esse apanhado geral, adentram-se em circunstâncias específicas relevantes para definir a possibilidade e a extensão do uso dos sistemas de identificação biométrica à distância em tempo real.

3.4. ASPECTOS TÉCNICOS – INEXISTÊNCIA DE NEUTRALIDADE

Ao apreciar os aspectos técnicos (e respectivos corolários) que circundam a identificação biométrica à distância em tempo real, um primeiro ponto a ser tratado é a questão da suposta neutralidade da tecnologia.

A ideia residiria no fato de que a tecnologia, por supostamente se basear em “aspectos técnicos”, seria neutra, isto é, não incorreria em vieses e padrões discriminatórios particulares da sociedade.

A ideia, contudo, é equivocada.

Em primeiro lugar, deve-se ter em mente que a tecnologia é política, na medida em que, já pelo seu próprio desenho, inclui certos interesses e exclui outros (Introna e Wood, 2004).

A título de exemplo, os autores citam a criação dos caixas bancários automáticos, feitos no intuito de facilitar o atendimento dos clientes, mas que possuem uma série de pressupostos para seu funcionamento, como o fato de que as pessoas terão acesso ao local onde situadas as máquinas, conseguirão enxergar, pressionar as teclas, lembrar da senha etc., o que, contudo, exclui uma parcela da sociedade (Introna e Wood, 2004).

A grande questão emerge quando as políticas de atuação das instituições passam a se guiar com base nas tecnologias criadas (que, por sua vez, ignoraram certos interesses); retornando ao exemplo dos caixas automáticos, percebe-se o potencial de aprofundamento de exclusões quando os bancos passam a pautar suas políticas na nova tecnologia (inicialmente com potencial de exclusão de pessoas com deficiência, como cegos e pessoas em cadeira de rodas) adotando medidas como fechamento de agências bancárias e cobrança de tarifas por transações com atendente humano, de modo que o que antes parecia uma “injustiça trivial” se multiplica para representar aparente estratégia intencional e coerente de exclusão (Introna e Wood, 2004).

Por isso, o caráter político da tecnologia vai além do artefato em si; este apenas funciona como um ponto de ligação numa rede técnico-social dinâmica, sustentada por uma multiplicidade de artefatos, acordos, alianças, convenções, procedimentos, em relações de poder e disciplina (Introna e Wood, 2004).

Não há, em verdade, como separar o puramente social do puramente técnico, pois ambos estão interligados (Introna e Wood, 2004).

Em tal cenário, o mito da objetividade, neutralidade, racionalidade e imparcialidade da aplicação de inteligência artificial foi gradualmente desconstruído (Pele e Mulholland, 2023).

De uma forma geral, Pasquinelli (2019) já demonstrou como os sistemas de inteligência artificial, por serem dependentes de dados de qualidade e carecerem de profundidade semântica, são passíveis de incorrerem em erros crassos e sujeitos a três tipos de vieses: sociais (os vieses

existentes na sociedade, decorrentes de desigualdades, serão internalizados pelo sistema por meio de aprendizado da máquina), de dados (o ato de coletar e formatar os dados têm o potencial de afetar a precisão da informação, carregando vieses em si) e algorítmico (é o aprofundamento dos vieses sociais e de dados pelo algoritmo, incrementando as desigualdades).

Assim, a tecnologia, programada pelo ser humano, não possui caráter automático de neutralidade (Daguer *et al.*, 2022). Conforme os autores: "é criado um ar de neutralidade, quando, na verdade, o algoritmo possui vieses para suas decisões e manutenção do estado de coisas violador de direitos fundamentais para determinados segmentos sociais*"* (Daguer *et al.*, p. 8). Segundo eles, especificamente na seara penal, a inteligência artificial teria o papel potencializador de seletividade do sistema criminal (Daguer *et al.*, 2022).

Especificamente em relação ao reconhecimento facial, Pele e Mulholland (2023) fornecem interessante exemplo acerca dos vieses discriminatórios em que a tecnologia, mesmo sem qualquer intenção do programador, pode incorrer. Os autores citam o exemplo de uma câmera Nikon adquirida por uma família taiwanesa em meados da década de 2010 com uma função para evitar fotografias com os olhos fechados (operada por tecnologia de reconhecimento facial), que se confundia ao interpretar que os membros da família estariam com os olhos fechados na fotografia, quando, em verdade, eles estavam com os olhos abertos, revelando vieses no desenvolvimento do produto, desenhado para caucasianos.

Percebe-se, portanto, que os passos anteriormente estudados acerca da implementação de sistemas de identificação biométrica à distância em tempo real devem ter em mente esse caráter político da tecnologia, que não é neutra.

Presente isso, impõe-se adentrar em alguns aspectos técnicos relevantes dos sistemas de identificação biométrica à distância em tempo real e correlacioná-los à estruturação de sistema hígido e condizente com direitos humanos.

Rememora-se que os sistemas de reconhecimento facial não oferecem resposta definitiva, mas meras probabilidades.

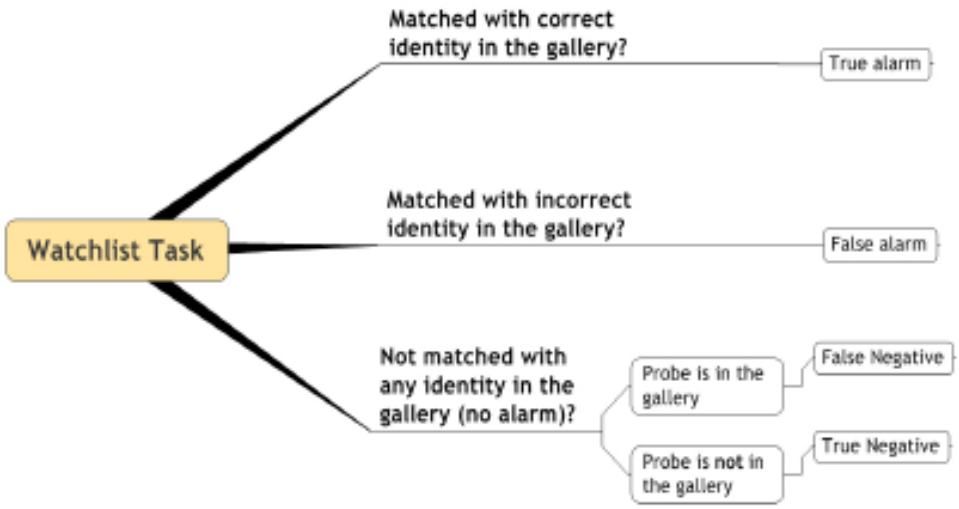
Logo, ao captar a face de determinado indivíduo, o sistema gerará um escore de similaridade com as imagens constantes no banco de dados; se o escore de similaridade com determinada imagem do banco de dados for superior à baliza estabelecida (*threshold*) haverá uma correspondência (Oliveira *et al.*, 2022).

Ao se estudar a baliza estabelecida (*threshold*), percebe-se que ela é intimamente ligada com a questão dos falsos positivos e falsos negativos.

Estes são as correspondências equivocadas feitas pelo sistema: quando uma pessoa é marcada como correspondente com a imagem, mas, na verdade, a imagem é de outra pessoa, isso é um falso positivo; por outro lado, quando uma pessoa não é marcada como uma correspondência, mas, na verdade, a sua imagem consta no banco de dados, isso é um falso negativo (Oliveira *et al.*, 2022).

Em caso de identificação biométrica à distância em tempo real, a situação é ilustrada pela seguinte figura:

Figura 5 – Possíveis resultados na atividade de lista de procurados



Fonte: Extraído de Introna e Nissenbaum (2010, p. 14).

E, nessas circunstâncias, conjugando-se falsos positivos e falsos negativos, há sempre um *trade-off*, pois, quanto maior for a baliza (*threshold*), maior será a possibilidade de falsos negativos, enquanto, ao se diminuir a baliza, aumentam-se os falsos positivos (Oliveira *et al.*, 2022; Introna e Nissenbaum, 2010). Isso exatamente pelo fato de que o escore de similaridade, a depender da baliza, será maior ou menor para gerar uma correspondência (Oliveira *et al.*, 2022; Introna e Nissenbaum, 2010).

Em razão disso, as taxas de incidência de um tipo de falso (positivo ou negativo) são determinadas a partir de uma taxa fixa para o outro tipo de falso: por exemplo, quantidade de falsos negativos com uma taxa de falso positivo de 1% (FRA, 2020).

Existe, então, evidente correlação com o nível de exigência de similaridade e o tipo de falso que o sistema encontrará (se positivo ou negativo).

Não bastasse, a situação se torna mais complicada em sistemas de identificação aberta (*open set identification*), como a identificação biométrica à distância em tempo real, em que o universo de pessoas cuja face captada não é determinável *a priori*. Assim, nesses sistemas abertos, a ausência de correspondência não significa necessariamente que a pessoa cuja face foi detectada não esteja no banco de dados, porém é inviável conferir tal circunstância em termos práticos (Introna e Nissenbaum, 2010).

O maior problema reside, portanto, na dificuldade em se computar os falsos negativos com os sistemas de identificação biométrica à distância em tempo real operando, já que as não correspondências não serão checadas individualmente para averiguar a precisão, e, assim, falsos negativos permanecem desconhecidos dos operadores (FRA, 2020).

Outro ponto a ser considerado é a quantidade de detecções de faces feita pelo sistema. Isso porque, ao haver grande número de detecções (em locais com grande movimentação, como, por exemplo, em metrôs), mesmo números pequenos de equívocos quanto a falsos positivos podem gerar, em termos absolutos, grande número de pessoas incorretamente identificadas e, portanto, cujos direitos fundamentais são afetados pelo mau funcionamento do sistema (FRA, 2020).

Sobre o tema, é importante destacar, ainda, que as chances de falsos positivos e falsos negativos são influenciadas por gênero e etnicidade (Fontes *et al.*, 2022).

Por esse motivo, a Agência da União Europeia para Direitos Fundamentais considera que os dados de precisão não podem ser calculados de forma geral, mas de acordo com diferentes grupos populacionais, dependentes de sexo, idade e grupos étnicos (FRA, 2020).

Cita-se um exemplo de aumento de precisão do sistema de identificação biométrica à distância em tempo real pela conjugação de três *softwares* distintos pela polícia de Berlim (FRA, 2020). Esse exemplo, todavia, possivelmente revela a fixação de balizas mais elevadas, exatamente pela conjugação de três sistemas distintos, de modo que ainda remanesce a questão do *trade-off* aqui analisada.

Logo, a questão da fixação das balizas representa, em si, uma forma de administração do risco, por implicar uma decisão política (Beck, 1992) a refletir a maneira de enfrentar o risco, pois determinará se o sistema será mais passível de falsos positivos ou falsos negativos.

Compreende-se, então, que o estabelecimento das balizas e o *trade-off* escolhido refletem uma decisão política ante o risco criado pela tecnologia de falsos positivos e falsos negativos, já que, tecnicamente, não há como escapar de tal escolha, pois a existência do risco é inerente à tecnologia de reconhecimento facial.

Então, esse aspecto vai além da mera escolha técnica e implica a consideração política e jurídica do impacto da decisão sobre direitos fundamentais e humanos afetados pela incidência dos erros da máquina cotejados com o propósito do sistema e sua eficiência em cumprir tal propósito.

Além da fixação da baliza para estabelecer se o sistema estará mais propenso a erros de falso positivo ou de falso negativo, outro aspecto técnico ligado à precisão do sistema diz respeito ao banco de dados utilizados.

Como assentado anteriormente (Fontes *et al.*, 2022), os sistemas de inteligência artificial (motor da identificação biométrica à distância em tempo real) dependem de dados (de qualidade) para ocorrência do processo de aprendizado pela máquina (*machine learning*). Quanto mais dados e de qualidade estiveram à disposição do sistema, melhor será o processo de aprendizagem e, então, melhor será o desempenho do sistema para realização da atividade proposta (FRA, 2020).

Aliás, a possibilidade de funcionamento dos sistemas de identificação biométrica depende de um banco de dados com imagens de indivíduos, a fim de que o algoritmo consiga traçar parâmetros para identificar uma face humana, diferenciá-la das demais imagens do ambiente e compará-la com o constante no banco de dados. Santos (2021, p. 219) bem elucida o ponto:

> Basicamente, o reconhecimento facial funciona com a seguinte metodologia: a inteligência artificial é treinada por meio de um banco de dados com várias imagens para extrair características específicas (como a distância do nariz aos olhos, da boca ao queixo, o formato do rosto, etc) e assim consegue identificar características biométricas das faces com base em padrões definidos.

De igual forma aponta a Agência da União Europeia para Direitos Fundamentais (FRA, 2020, p. 10, tradução nossa):

> O software de reconhecimento facial é baseado em modelos pré-treinados, o que significa que o software desenvolve regras para identificação de rostos com base em um banco de dados de imagens faciais. Isto foi possível através do aumento da disponibilidade de imagens faciais com maior qualidade e o aumento no poder de computação para processar grandes quantidades de dados. Do ponto de vista dos direitos fundamentais, é importante saber quais conjuntos de dados foram usados para construir o facial software de reconhecimento, pois isso influencia o desempenho do software.

Não apenas o tamanho do banco de dados importa, mas também as características das imagens que nele constam.

Conforme assentam Introna e Nissenbaum (2010), o sucesso do sistema de reconhecimento facial é criticamente dependente das características da galeria constante no banco de dados, como qualidade da imagem, tamanho e idade. A qualidade da imagem seria, ao ver dos autores, uma das variáveis mais importante para o sucesso do sistema de reconhecimento facial (Introna e Nissenbaum, 2010, p. 39).

Consoante indicado por Duarte *et al.* (2021), aspectos ligados à qualidade da imagem, como desobstrução da face e suas estruturas, além de resolução e nitidez, são requisitos absolutos para possibilitar o exame de comparação facial. Assim, imagens que não atendam a parâmetros mínimos de desobstrução da face, suas estruturas e de resolução e nitidez são imprestáveis para subsidiar análises técnicas de comparação de face (Duarte *et al.*, 2021).

Consequentemente, se o banco de dados não observar esses critérios mínimos de qualidade das imagens, certamente o processo de aprendizagem do algoritmo acontecerá de forma enviesada e pautada em dados ruins, resultando em falta de precisão e inocuidade do sistema para cumprir suas finalidades, pois incorrerá em diversas correspondências falsas.

Não bastasse, há diversos outros aspectos relacionados com a qualidade da imagem, como iluminação, contraste, similaridade, contemporaneidade, que, embora não inviabilizem, *a priori*, uma comparação facial, são importantes para maior precisão do exame (Duarte *et al.*, 2021).

Nessa senda, a Agência da União Europeia para Direitos Fundamentais (FRA, 2020) pontua que diversos fatores influenciam a qualidade das imagens, como oclusão do fundo e do objeto, iluminação e reflexão da luz, ergonomia, idade, envelhecimento, gênero, cor da pele e condições da pele. Há, então, uma multiplicidade de fatores a garantir que as imagens constantes no banco de dados para treinamento do algoritmo sejam de qualidade.

Logo, não basta observar, na construção do banco de dados, um parâmetro mínimo de quantidade, mas também deve ser buscado o melhor padrão de qualidade para as imagens que vão compor referido banco, de acordo com o desenho do algoritmo. Relembrando: ao se estudar as fases de implementação do sistema de inteligência artificial, observou-se que, após a concepção do desenho do algoritmo, será montado o banco de dados em conformidade com tal concepção; no caso, ao se trabalhar com identificação biométrica à distância em tempo real, ao se conceptualizar o algoritmo de inteligência artificial, deve ser estabelecido o padrão de imagens a compor o banco de dados constante no sistema, no intuito de garantir que o processo de aprendizagem da máquina ocorra da melhor forma possível.

A qualidade das imagens, por sua vez, não representa parâmetro único, mas depende de representatividade de diferentes grupos demográficos.

O maior número de dados utilizados pelo sistema lhe possibilidade fornecer resultados mais precisos; todavia, não apenas a quantidade de imagens é relevante (e sua qualidade em geral), mas também a representatividade das imagens é condição básica para sucesso do sistema (Fontes *et al.*, 2022).

Assim, a coleta inadequada de dados pode significar insuficiente representação de grupos particulares, a resultar em vieses desfavoráveis a grupos minoritários (Fontes *et al.*, 2022).

Por esse prisma, qualidade não envolve um padrão geral das fotografias constantes no banco de dados, mas também a representatividade constante no banco de dados, o que está diretamente ligado ao assunto relativo a vieses.

Inclusive, acerca da qualidade das imagens e representatividade, Wu *et al.* (2023), em estudo inovador sobre o tema, analisam a específica correlação entre a luminosidade da imagem e a tonalidade da pele para fins de precisão do reconhecimento facial, e chegam à conclusão de que diferentes tons de pele dependem de diferentes graus de luminosidade para maior precisão do sistema.

Os autores infirmam a ideia de que “quanto maior luminosidade na imagem, maior será a precisão na identificação”, ao demonstrar que diferentes tons de pele dependem de diferentes cenários de luminosidade para maior precisão do sistema (Wu *et al.*, 2023).

Os padrões de luminosidade são distintos entre homens e mulheres e, sobretudo, entre caucasianos e afro-americanos (Wu *et al.*, 2023).

Diante disso, a definição da qualidade das imagens não depende apenas de englobar grupos demográficos distintos; as próprias fotografias desses grupos demográficos devem respeitar a etnia deles quanto à melhor forma de representação da imagem no sistema para maior precisão. Aqui, relembra-se o exemplo fornecido por Pele e Mulholland (2023) da família taiwanesa cuja fotografia não era captada por uma câmera Nikon, que confundia a face dos membros da família como se estivessem de olhos fechados. Esse exemplo singelo, se extrapolado para universo indefinido de pessoas que ficarão sujeitas à identificação biométrica em tempo real, revela os perigos da tecnologia, na medida em que falhas na representatividade do banco de dados tenderão a fomentar equívocos do sistema, impulsionados pela aprendizagem da máquina, a causar maiores vieses e falhando no objetivo proposto.

Portanto, a construção de um banco de dados de qualidade impõe não apenas uma qualidade geral das imagens e adequada representatividade, mas também que os parâmetros de qualidade das imagens estejam de acordo com os diferentes grupos demográficos, separados por gênero, etnia, tons de pele e idade, já que determinados parâmetros, como luminosidade, não serão idênticos entre todos os grupos (Wu *et al.*, 2023).

Um último ponto relevante sobre o banco de dados diz respeito à sua origem.

Como visto, do ponto de vista técnico, o maior número de imagens aumenta a capacidade de aprendizado do sistema, a levar, em tese, a maior precisão.

Acontece que, ao se coletar mais dados para aprimorar os bancos de dados a alimentar o sistema, aumenta-se o risco de intrusão em direitos individuais, notadamente de privacidade (Fontes *et al.*, 2022).

Essa questão assume especial relevância ao se ter em mente que a utilização do sistema se direciona para persecução criminal, em que se está em jogo a liberdade dos indivíduos e se busca medidas de freios e contrapesos para evitar arbitrariedades estatais. Ao se aplicar o sistema para esfera penal, maiores precauções devem ser observadas no intuito a não ensejar excedente intromissão na vida dos particulares a desembocar em cenário de supervigilância estatal em face dos indivíduos (Oliveira *et al.*, 2022).

Portanto, a questão da coleta de imagens é especialmente relevante não apenas pela direta correlação com a precisão do sistema, mas também porque as imagens coletadas são passíveis de figurarem na lista de procurados para fins penais e resultarem na restrição de direitos, de modo a emergir questões relativa ao campo da privacidade dos indivíduos (Fontes *et al.*, 2022).

Inclusive, são diversos autores que apontam ser inadmissível a utilização de uma série de imagens colhidas de forma precária (como de redes sociais) para compor o banco de dados de sistemas de reconhecimento facial, o que levaria à vigilância de massas e severas intromissões em direitos individuais (Smith e Miller, 2022; Hirose, 2017; Fontes *et al.*, 2022).

Sobre o ponto, aliás, Hirose (2017) aponta grande preocupação pela construção de bancos de dados destinados ao reconhecimento facial compostos por imagem de pessoas sequer condenadas por qualquer crime, o que levaria, segundo ele, a indagações acerca de precisão, justiça e vieses raciais de tal prática, tendente a afetar desproporcionalmente determinados grupos étnicos.

A questão é tormentosa, na medida em que, ao mesmo tempo que o sistema de identificação biométrica à distância em tempo real necessita de robustez de dados de qualidade para operar de forma precisa, a coleta de forma ampla de dados pelo governo cria preocupações quanto à privacidade dos indivíduos, que seria ameaçada pelo potencial de vigilância em massa e práticas arbitrárias pelo Estado.

Nesse contexto, o projeto TELEFI (*Towards the European Level Exchange of Facial Images*)[6], desenvolvido pela União Europeia para avaliar como o reconhecimento facial está sendo utilizado no bloco para investigação de crimes, analisou as bases de dados utilizadas pelos países componentes do referido bloco.

Segundo constatado na referida pesquisa, os países da União Europeia não apresentam uniformidade quanto aos bancos de dados e coleta de dados para construção dos sistemas de reconhecimento facial (TELEFI, 2021).

A aquisição de dados, conforme tal estudo, pode ser dividida em duas classes de banco de dados: criminais – oriundos da resolução de crimes – e civis – originados por diferentes procedimentos, como confeccionar carteira de identidade, obter carteira de motorista, ingresso no território como estrangeiro etc. (TELEFI, 2021).

A coleta de banco de dados civis varia significativamente entre os Estados-Membros, de modo que uma generalização da informação não foi possível (TELEFI, 2021).

Contudo, a aquisição de imagens pelos bancos de dados criminais envolve muitos aspectos comuns entre os países (TELEFI, 2021). Em geral, as imagens são capturadas pelas

---

6 Disponível em: https://www.telefi-project.eu/. Acesso em: 15 dez. 2024.

forças policiais sob as mais variadas premissas, juntamente com dados não biométricos (TELEFI, 2021). Na maioria dos países, os dados coletados são diretamente cadastrados no sistema pela própria polícia, à exceção dos Países Baixos, Grécia, Chipre e Croácia, em que as fotografias são enviadas a outros órgãos para serem inseridas no sistema (TELEFI, 2021).

Não há, então, um padrão único para construção do banco de dados que alimentará o sistema de identificação biométrica à distância em tempo real; novamente cuida-se de aspecto que vai além da mera escolha técnica e implica a consideração política e jurídica do impacto da decisão sobre direitos fundamentais e humanos afetados.

Sobre o ponto, quanto à composição do banco de dados em si, o Brasil já utiliza o ABIS (Solução Automatizada de Identificação Biométrica)[7], de modo que poderia se cogitar a utilização do mesmo banco de dados para fins de identificação biométrica à distância em tempo real. Contudo, tendo em vista que a incidência do sistema de identificação biométrica à distância em tempo real pode ser muito mais significativa, com potencial para atingir um número muito maior de pessoas, além das necessidades de aprendizado do algoritmo, inclusive com representatividade e padrões específicos de qualidade de imagem para diferentes demográficos, parece prudente refletir sobre a melhor forma de construção do banco de dados a partir uma análise individualizada dos riscos específicos de tal tecnologia, sem generalizações.

Logo, a construção do banco de dados, com imagens de qualidade, representativas, com padrões específicos para diferentes grupos demográficos, e cuja coleta respeite direitos individuais e da coletividade, reflete fator dependente da ponderação de riscos e de decisão política e jurídica sobre impacto em direitos fundamentais e humanos da população envolvida.

Isso tudo indica que a coleta de fotografias deve ocorrer de forma criteriosa, com parâmetros já visando à atividade de identificação biométrica à distância em tempo real, sob pena não apenas de ineficiência e viés do sistema, mas da construção de toda uma base de dados com infringência à privacidade dos indivíduos que não detenham correlação com crimes. Ainda que se queira alargar a base de dados para englobar base de dados civis – como acontece em determinados países da Europa (TELEFI, 2021) – a questão deve ser submetida à análise de ponderação específica para sopesar os riscos e os benefícios dessa decisão política com íntimos impactos na esfera jurídica da população.

---

7 **BRASIL. Polícia Federal.** Polícia Federal implementa nova solução automatizada de identificação biométrica. Disponível em: https://www.gov.br/pf/pt-br/assuntos/noticias/2021/07/policia-federal-implementa-nova-solucao-automatizada-de-identificacao-biometrica. Acesso em: 15 dez. 2024.

Feita essa análise sobre o banco de dados, adentra-se no aspecto mais polêmico da referida tecnologia, constante na existência de vieses em prejuízo a determinados grupos demográficos.

Retomando o anterior exemplo da câmera Nikon que não reconhecia os olhos abertos de uma família taiwanesa, as tecnologias de reconhecimento facial desde os primórdios apresentam índices de falhas distintos a depender do grupo demográfico analisado.

A precisão do reconhecimento facial depende do grupo demográfico do indivíduo analisado.

Introna e Wood (2004), ao analisar os resultados do teste "Vendor" de 2002, apontaram diferentes níveis de precisão a depender da origem demográfica, indicando que o reconhecimento facial funciona melhor em homens do que em mulheres, e melhor em asiáticos e afro-americanos do que em caucasianos[8]. Nesse contexto, Introna e Wood (2004, p. 192) questionam que a maior precisão no reconhecimento de pessoas distintas dos caucasianos geraria mais correspondências e possíveis falsos positivos a prejudicar tais populações.

Apesar da evolução da tecnologia, não se logrou eliminar a existência de vieses em detrimento de determinados grupos demográficos.

Em celebrado estudo denominado "Gender Shades", Buolamwini e Gebru (2018) revelaram que todos os sistemas de reconhecimento facial cujo desempenho foi avaliado em quatro grupos distintos (mulheres de pele mais escura, mulheres de pele mais clara, homens de pele mais escura e homens de pele mais clara) ostentavam maior precisão em homens e em tons de pele clara, de modo que o pior resultado se relacionava à precisão na identificação do rosto de mulheres negras.

Aqui desponta o conceito de discriminação interseccional, segundo o qual a "presença simultânea de fatores diversos de diferenciação injusta e prejudicial produz novas e originais formas de discriminação, desafiando a formulação de respostas jurídicas apropriadas" (Rios e Silva, 2015, p. 11).

Nessa senda, a mulher negra enfrenta falha do algoritmo por dois fatores de discriminação distintos: gênero e raça, a acentuar a injustiça contra ela decorrente da falta de precisão no reconhecimento de sua face.

---

8 Note-se que se trata de tecnologia distinta da inteligência artificial, cujos vieses, como serão explorados, tendem a ser menos precisos na população com tons de pele mais escuro.

Como o estudo “Gender shades”, há diversos outros exemplos de vieses decorrentes da falta de precisão do reconhecimento facial de grupos minoritários a incrementar tratamento injusto, notadamente à população negra (Smith e Mann, 2024).

Inclusive, relatório do Instituto Nacional de Padronização e Tecnologia dos Estados Unidos da América (*National Institute of Standards and Technology – NIST*) de 2019 apontou a menor precisão para reconhecimento de afro-americanos e asiáticos, ao indicar que essas raças teriam de 10 a 100 vezes mais chances de serem má-identificadas (Smith e Mann, 2024).

Visto que a tecnologia é política e que as inteligências artificiais são dependentes de dados de qualidade, não são surpreendentes diferentes níveis de precisão do algoritmo em face de distintos grupos demográficos quando não são dedicados esforços para mitigação de vieses.

Aliás, “o algoritmo é treinado para seguir os padrões presentes no seu banco de dados e, na maioria das vezes, é eivado de vieses que são percebidos na sua aplicação diante de consequências preconceituosas, como a mencionada por Joy Buolamini*”* (Santos, 2021, p. 226).

Como bem salientam Pele e Mulholland (2023, p. 177, tradução nossa):

> [...] pesquisas mostram que a existência de vieses na cultura humana é inevitavelmente replicada na tecnologia, pois os vieses reproduzem, em grande escala, os preconceitos e estereótipos que negativamente afetam a mediação entre humano e máquina.

Certamente os vieses do reconhecimento facial são ainda mais nefastos no campo criminal, porquanto apresentam potencial de perpetuar discriminação contra minorias e exacerbar a seletividade do sistema penal (Santos, 2021).

Introna e Nissenbaum (2010) sinalizam que a existência de vieses do sistema de reconhecimento facial a aumentar número de falsos positivos em prejuízo a determinados grupos minoritários enseja a abordagem desproporcional de tal população, em circunstância semelhante ao perfilamento racial, de modo a se tornar um mecanismo de injustiça social.

É importante destacar, ainda, que os sistemas de identificação biométrica à distância em tempo real, uma espécie do gênero tecnologia de reconhecimento facial, apresentam índices ainda mais baixos de precisão (FRA, 2020). Isso porque o ambiente de coleta das imagens não pode ser controlado (ao contrário de outras tecnologias de reconhecimento facial, como controle

de fronteiras), estando sujeitos a fatores variáveis de luminosidade, distância e posição, a potencializar a ocorrência de falsos (FRA, 2020).

Logo, a questão dos vieses assume ainda mais relevância ao se tratar da identificação biométrica à distância em tempo real, na medida em que tal tipo de sistema, por operar em ambiente não controlado, está, por si só, sujeito a menores índices de precisão.

Os vieses podem ocorrer em diversas etapas da criação do sistema de inteligência artificial, seja no desenho, teste ou implementação do algoritmo, de forma consciente ou não (FRA, 2020).

Em tal toada, um dos pontos principais diz respeito aos dados que serão alimentados no sistema, pois, a depender da forma de coleta e categorização de dados, os vieses prejudiciais dos designers humanos serão convertidos em viés algorítmico (Dushi, 2020).

Assim, os designers dos sistemas de reconhecimento facial devem ter conhecimento da temática para não acentuar vieses já existentes no sistema de justiça criminal (Smith e Mann, 2023).

Isso porque, ao se considerar que as minorias já são desproporcionalmente escrutinadas pelas forças de segurança pública e sobre-representadas no sistema de justiça criminal, a falta de precisão representa fator a incrementar padrões discriminatórios (Smith e Mann, 2024).

Além da questão da falta de precisão do algoritmo quanto a determinados grupos demográficos, outro ponto é relevante para aplicação da tecnologia sob a perspectiva de justiça social.

Trata-se da localização das câmeras, que, a depender da área, podem provocar vigilância exacerbada sobre determinadas populações, incrementando padrões de tratamento discriminatório (Smith e Mann, 2024).

Fontes *et al.* (2022) apontam que autoridades poderiam ser mais suscetíveis a colocar as câmeras em áreas com maior índice de criminalidade, o que, a seu turno, geraria maiores índices de prisões em tais locais, aumentando, consequentemente, a vigilância, de modo a aprofundar a estigmatização de determinadas comunidades e afetar desproporcionalmente seus residentes.

Em exemplo prático dessa estigmatização pelo posicionamento das câmeras, Najibi (2020) cita o Projeto Luz Verde (*Project Green Light – PGL*) da cidade de Detroit, calcado na instalação de câmeras de alta definição, que foram direcionadas para regiões habitadas pela população negra, evitando áreas com caucasianos e asiáticos.

Segundo o autor (Najibi, 2020), o posicionamento das câmeras, tornando as áreas vigiadas de forma exacerbada, causou diversos prejuízos à população local, aprofundando desigualdades.

Assim, não apenas a falta de precisão do algoritmo, mas a escolha do local a colocar as câmeras, são fatores que podem causar a ocorrência de prejuízo a determinados grupos demográficos, relembrando-se, no ponto, o conceito de discriminação interseccional, caso a tecnologia opere de forma a acentuar discriminações já existentes na sociedade e, assim, aprofundar desigualdades.

Certamente não é isso que se busca na implantação desses sistemas de identificação biométrica em tempo real (que visam a trazer proveitos para segurança pública), de modo que esforços devem ser empreendidos para se eliminar os efeitos de mencionados vieses.

Apesar das contundentes críticas aos vieses dos sistemas de reconhecimento facial, Smith e Mann (2024) não se posicionam pelo banimento da tecnologia, mas advogam pelo enfrentamento das próprias desigualdades e discriminações estruturais refletidas no algoritmo; por essa perspectiva, a tecnologia não seria o problema, nem a solução, impondo-se, em verdade, a necessidade de representatividade social nos dados utilizados e que não haja utilização exacerbada da tecnologia em áreas de concentração de minorias (Smith e Mann, 2024).

Inclusive, a existência de auditorias éticas regulares é ponto fundamental para construção de um sistema mais equânime.

Logo, a forma de enfrentar os vieses não seria pela eliminação da tecnologia em si, mas na preocupação em construir um sistema atento a tal questão, capaz de operar com mecanismos a corrigir falhas decorrentes de vieses, sobretudo os prejudiciais a grupos minoritários.

Não custa relembrar, por exemplo, a pesquisa de Wu *et al.* (2023), no sentido de que a maior precisão do reconhecimento facial depende do ajuste de luminosidade de acordo com o tom de pele, a revelar que não haveria padrões gerais de imagem ideal, mas, sim, padrões de acordo com o grupo demográfico a ser representado.

Isso revela preocupação na construção de uma tecnologia equânime, focada na eliminação de vieses prejudiciais, sobretudo a grupos minoritários, o que passa por todo o ciclo de vida da inteligência artificial, desde a concepção até a revisão, com gatilhos específicos para detectar mau funcionamento decorrente de falhas de precisão em detrimento de grupos demográficos.

Presente que, já do ponto de vista técnico, os sistemas de identificação biométrica à distância em tempo real estão sujeitos a falhas e vieses, principalmente em face de determinados grupos demográficos, torna-se evidente que o sistema não pode operar de forma totalmente autônoma e automática.

Aliás, como visto no ciclo de vida da inteligência artificial, os sistemas são objeto de monitoramento e revisão, o que, por si só, já revela que a inteligência artificial não deve operar sem supervisão humana (Floridi *et al.*, 2018).

Logo, em termos gerais, ainda que haja delegação de importantes tarefas à inteligência artificial, pelo menos parte do funcionamento do sistema deve continuar sob supervisão humana (Floridi *et al.*, 2018).

Nessa senda, Floridi *et al.* (2018, p. 693, tradução nossa) assinalam a necessidade de permanência da supervisão humana, apesar da tendência cada vez maior de o sistema de inteligência artificial operar de forma autônoma:

> Cada vez mais, talvez não precisemos estar "por dentro" (isto é, como parte do processo ou pelo menos no controle dele), se pudermos delegar nossas tarefas para IA. No entanto, se confiarmos na utilização de tecnologias de IA para aumentar as nossas próprias habilidades de maneira errada, podemos delegar tarefas importantes e, acima de tudo, decisões a sistemas autônomos que devem permanecer, pelo menos parcialmente, sujeitos à supervisão humana. Isto, por sua vez, pode reduzir a nossa capacidade de monitorar o desempenho desses sistemas (por não estarem mais "por dentro") ou prevenindo ou corrigindo erros ou danos que surgem ("pós-loop"). Também é possível que estes danos potenciais podem se acumular e se consolidar, à medida que mais e mais funções são delegadas para sistemas artificiais. É, portanto, imperativo encontrar um equilíbrio entre a prossecução das ambiciosas oportunidades oferecidas pela IA para melhorar a vida humana e o que podemos alcançar, por um lado, e, por outro, garantir que continuamos no controle destes grandes desenvolvimentos e dos seus efeitos.

Assim, os autores, ao tratar de sistemas de inteligência artificial em geral, concluem ser necessário encontrar um balanço entre as oportunidades oriundas da operação autônoma de tais sistemas e a garantia de permanência do controle humano, no intuito de evitar potenciais danos decorrentes da delegação de tarefas à inteligência artificial (Floridi *et al.*, 2018).

Se a necessidade de manutenção de supervisão humana é pressuposto das inteligências artificiais em geral, isso é ainda mais presente no caso de sistemas de identificação biométrica

em tempo real destinados à segurança pública, pelo risco de falhas e vieses, aliado à finalidade altamente relevante e sensível.

Nesse sentido, como bem coloca Raposo (2022), a legislação a regular o reconhecimento facial em segurança pública deve, em regra, banir decisões tomadas de forma automática a partir do resultado do sistema.

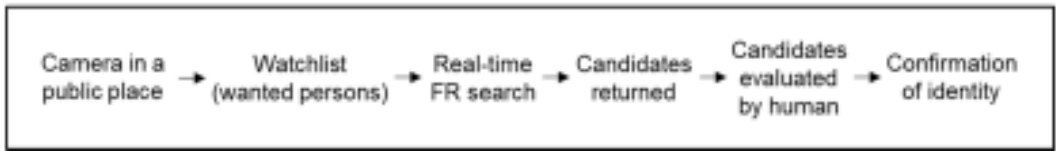
Qualquer potencial correspondência deve ser confirmada por um operador humano para evitar falsos positivos (Raposo, 2022).

A supervisão humana, ainda, deve representar uma avaliação autônoma e não apenas uma confirmação cega do resultado fornecido pela tecnologia (Raposo, 2022).

O operador humano deve confirmar a similaridade entre a face detectada pelo sistema de inteligência artificial e aquela constante no banco de dados.

Ao descrever as etapas de funcionamento do sistema de identificação biométrica à distância em tempo real, o Projeto TELEFI (2021, p. 25) assim descreve:

Figura 6 – Reconhecimento facial em tempo real



Fonte: Extraído de Projeto TELEFI (2021, p. 25).

Como se vê, na identificação biométrica à distância em tempo real, quando a câmera capta uma face cuja correspondência é marcada como positiva pelo sistema, cabe a um operador humano avaliar o resultado da operação para confirmar o positivo (TELEFI, 2021). Portanto, o acionamento das forças policiais para abordagem da identificação da pessoa somente ocorrerá após o resultado ser confirmado pelo operador humano.

Dessa maneira, o sistema não operará de forma completamente autônoma, o que reduz potenciais falhas.

É fundamental, ainda, que o operador humano responsável pela supervisão do resultado detenha conhecimentos na forma de funcionamento do sistema de identificação biométrica; é

dizer, deve ser pessoa capaz de identificar a ocorrência de falsos positivos e vieses, nos termos explicados anteriormente.

Esse aspecto técnico do funcionamento da identificação biométrica à distância em tempo real, a saber, a supervisão humana, é essencial para evitar falhas, sobretudo em sistema que opera em ambiente não controlado (FRA, 2020). O operador humano, ao analisar o resultado obtido pelo sistema, ante seus conhecimentos, poderá identificar fatores de potencial confusão da máquina, como, por exemplo, face detectada em imagem de baixa qualidade (pela posição, luminosidade, encoberta, entre outros fatores), grupos demográficos de menor precisão e outras situações da detecção a causarem dúvidas na correspondência.

Os conhecimentos técnicos do operador humano direcionam-se ao funcionamento da inteligência artificial e não particularmente à segurança pública (sem prejuízo, de qualquer sorte, da conjugação de ambos, o que seria ainda mais benéfico).

Eventuais dúvidas despertadas no operador humano acerca da idoneidade da correspondência obtida pelo sistema de inteligência artificial podem ensejar que se aguarde na realização da abordagem para uma confirmação mais segura (por exemplo, captação da face por uma nova câmera no ambiente), tudo a depender do contexto.

Portanto, a supervisão humana é importante fator a evitar que os sistemas de identificação biométrica à distância em tempo real operem de forma descontrolada, com potenciais a diversos falsos positivos e vieses, em prejuízo a grupos demográficos específicos, notadamente a população negra. Embora não seja uma solução por si, trata-se de relevante peça no funcionamento a fim de garantir a construção de um sistema mais equânime, justo e com medidas para mitigar a ocorrência de falsas correspondências e vieses.

3.5. INTERSECÇÕES COM DIREITOS HUMANOS

O exposto até aqui permite identificar que a utilização de identificação biométrica em tempo real levanta relevantes questões acerca da proteção de direitos humanos.

Essas questões serão detalhadas no presente capítulo.

De qualquer forma, é interessante abordar brevemente alguns critérios gerais sobre a interferência em direitos humanos decorrente do uso de inteligência artificial.

Em estudo sobre o tema, Kriebitz e Lütge (2020) sintetizam as interferências em direitos humanos mediante três princípios: consenso, prevenção de dano e proporcionalidade.

Em um primeiro momento, a interferência na esfera do indivíduo seria admitida mediante seu consenso, que legitimaria eventual invasão em alguma seara abstratamente protegida por direito humano (Kriebitz e Lütge, 2020).

Ainda assim, haveria situações em que se admite interferência na esfera do indivíduo sem o respectivo consenso, quando a interferência se justifica para evitar danos a terceiros. É a partir desse princípio que os direitos humanos assumem feição de prestações positivas a vincular instituições e terceiros (Kriebitz e Lütge, 2020).

Acontece que a interferência deve ser proporcional ao dano evitado, do que deriva a ideia de igualdade perante a lei (Kriebitz e Lütge, 2020). Existem casos, contudo, que o princípio da proporcionalidade não é aplicável, pois determinados direitos humanos, como proibição à tortura e à escravidão, são inderrogáveis (Kriebtiz e Lütge, 2020).

Ao aplicar tais princípios à identificação biométrica à distância em tempo real, Fontes e Perrone (2021) apontam que a aplicação da proporcionalidade deve ponderar os problemas sociais existentes com aqueles que podem surgir a partir da aplicação do novo sistema como forma de solução.

Na ponderação principiológica sobre a identificação biométrica à distância em tempo real, necessita-se de juízo probabilístico sobre os potenciais desdobramentos da utilização da tecnologia, haja vista todos os aspectos técnicos anteriormente traçados, que envolvem a autonomia e a opacidade do sistema, contínuo aprendizado, dependência de dados, *trade-off* de falsos positivos e falsos negativos, além de vieses.

Portanto, a ponderação para analisar o uso da tecnologia e seu impacto com direitos humanos depende desse olhar minucioso.

Por conta disso, esmiuçam-se as principais intersecções com direitos humanos.

O primeiro ponto a chamar atenção diz respeito à potencial violação do direito à privacidade pelo sistema de identificação biométrica à distância em tempo real. Dentro dessa discussão se insere o direito à proteção dos dados individuais, apesar de serem direitos distintos, ainda que estritamente correlacionados (FRA, 2020).

A privacidade é um conceito em constante evolução, uma vez que se trata da representação cultural do que é consentido e socialmente aceito de ser compartilhado em determinados contextos e esferas (Fontes e Perrone, 2021).

A primeira concepção de privacidade, ainda do século XIX, representaria conceito negativo, no sentido do direito em ser deixado só (Santos, 2021). O decurso do tempo e a evolução social impuseram atualização de tal conceito, que passou a "abarcar desenvolvimento e livre exercício do direito de personalidade" (Santos, 2021, p. 218).

Por esse prisma, o direito à privacidade reflete esfera jurídica protegida para possibilitar o desenvolvimento do indivíduo. Segundo Smith e Miller (2022), a privacidade se relacionaria profundamente com o valor da autonomia do indivíduo, destacando que, para o indivíduo buscar seus projetos pessoais, é necessário algum grau de privacidade.

Sob o prisma individual, incluem-se a privacidade espacial e informacional (Lynch, 2024).

Além da esfera individual, a privacidade também pode ser coletiva (Lynch, 2024).

Nesse sentido, a privacidade transpõe a expectativa subjetiva e impacta valores sociais (Lynch, 2024), o que revela a natureza objetiva do direito.

Exatamente por essa perspectiva, a discussão sobre a interferência no direito à privacidade não pode ficar adstrita aos indivíduos efetivamente afetados, na medida em que o potencial de interferência pode atingir o valor social da privacidade em si.

Em tal toada, Fontes *et al.* (2022, p. 06, tradução nossa) alertam que "a privacidade é um valor social cuja perda representa uma armadilha". Isso porque a perda da privacidade na perspectiva de valor social coloraria em risco a própria democracia (Smith e Miller, 2022).

As tecnologias de reconhecimento facial, por si, já representam intromissão no direito à privacidade individual ao conectar uma imagem facial a uma identidade, realizando correlação com outra informação constante na base de dados do sistema (Introna e Nissenbaum, 2010).

Ante o caráter intrusivo da identificação biométrica à distância em tempo real, referido sistema teria potencial para "eviscerar a privacidade como a conhecemos" (Hirose, 2017, p. 1593, tradução nossa), em razão do potencial uso para escanear a face de diversas pessoas sem qualquer suspeita individualizada.

Fontes *et al.* (2022) destacam que o sistema pelo qual a face de todo indivíduo que passe pelo local é analisada representa a existência de vigilância sem prévia suspeita da prática de crime, com exposição ao potencial acionamento da polícia a partir do resultado obtido.

Nessa linha, Fontes *et al.* (2022, p. 10, tradução nossa) bem esclarecem os perigos potenciais da identificação biométrica à distância no exercício de liberdades individuais:

> A adoção de sistemas de vigilância alimentados por IA expõe as populações a risco aumentado de desequilíbrio de poder, baseado na possibilidade de acesso a informações privilegiadas sobre a vida privada dos indivíduos coletadas deles e alimentando os sistemas para fornecer informações às autoridades públicas. Enquanto informações de saída podem ser extremamente relevantes para prever, prevenir e neutralizar ameaças sociais, ultrapassa os limites da privacidade pessoal e confere quantidade imensa de poder às autoridades públicas sobre indivíduos, o que pode levar ao enfraquecimento dos valores democráticos e direitos e liberdades individuais.

O fato de o sistema operar em espaço público não seria justificativa para afastar o referido direito, eis que isso não infirma a legítima expectativa de privacidade em determinados contextos (Lynch, 2024).

Em verdade, os limites do direito à privacidade são incertos, dependendo do contexto para sua concretização (Smith e Miller, 2022).

Adotando o conceito sociológico de desatenção civil[9], Hirose (2017) defende a existência de um direito à privacidade no espaço público, entendendo que a aplicação de sistemas de identificação biométrica sem qualquer tipo de limite representaria violação a tal direito, contrário à Constituição dos Estados Unidos, notadamente à Quarta Emenda.

A Agência da União Europeia para Direitos Fundamentais expõe que a Corte Europeia de Direitos Humanos já assinalou a existência de circunstâncias de legítima expectativa de privacidade do indivíduo no espaço público, sem ser submetido à vigilância (FRA, 2020).

Consequentemente, a aplicação irrestrita da identificação biométrica à distância em tempo real causaria impacto negativo na privacidade dos indivíduos.

---

9 Cuida-se temática desenvolvida pelo sociológico Erving Goffman, calcada, de forma extremamente resumida, na ideia de que a convivência social em espaços públicos se funda em um consenso de que os indivíduos assumem consciência da presença uns dos outros, sem, todavia, depositar atenção excessiva ou representar alguma ameaça, o que prejudicaria a convivência social e o trânsito em espaços públicos.

Por outro lado, o fato de o sistema de identificação biométrica em tempo real interferir na privacidade dos indivíduos não é suficiente para justificar a sua não utilização, já que, cuidando-se de tecnologia destinada à consecução da segurança pública, atividade estatal que também representa direito fundamental e humano da população contra a prática delitiva, cabe o balanceamento dos benefícios e malefícios para tomada de uma decisão em prol do melhor desenvolvimento social.

Conforme bem sinalizam Daguer *et al.* (2022, p. 02): "na difícil compatibilização entre intimidade e/ou privacidade e segurança pública, cabe ao Estado estabelecer o equilíbrio para o livre desenvolvimento da sociedade".

O aspecto crucial, então, é determinar o ponto em que a esfera da privacidade pode ser infringida por razões de segurança pública, o que está relacionado com as finalidades do sistema (Smith e Miller, 2022). Os autores apontam (Smith e Miller, 2022, p. 172, tradução nossa):

> Utilizar, então, a tecnologia de reconhecimento facial para investigar um crime grave, como um homicídio ou rastrear um suspeito terrorista, se conduzido sob ordem judicial, é certamente eticamente justificado. Por outro lado, a vigilância intrusiva de um suspeito de furto não relevante possivelmente não será justificada.

Em suma, a interferência no direito à privacidade é inerente à aplicação da identificação biométrica em tempo real, eis que o sistema implica reiterado monitoramento das faces detectadas, devendo-se encontrar a medida em que justificável tal interferência, a partir dos objetivos buscados pelo sistema. Logo, em casos de situações mais graves ou extremas, o valor da segurança pública assumiria relevância ante a privacidade, justificando o afastamento da incidência de tal direito.

Outro aspecto atinente ao gênero privacidade revolve o direito à proteção dos dados individuais.

Como abordado, a construção do sistema de identificação biométrica depende da coleta e da categorização de dados em um banco de dados. No caso, os dados são pessoais e sensíveis, por revolver a biometria facial da pessoa, (FRA, 2020; Goldenfein, 2024), o que está de acordo com o conceito fornecido no art. 5º, I, da LGPD.

Ao se considerar que os dados destinados à formação do banco de dados são pessoais e sensíveis, isso implica maior rigor jurídico na coleta, processamento e armazenamento (FRA,

2020). Consequentemente, em casos de coleta de indevida, o uso será ilegal (FRA, 2020; Dushi, 2020).

Em regra, a utilização dos dados sensíveis é possível mediante consenso, nos termos, grosso modo, do princípio geral explorado por Kriebitz e Lütge (2020); todavia, na esfera da segurança pública, não há como esperar o consenso individual (FRA, 2020), seja por uma questão de que os alvos do sistema não estarão dispostos a se auto incriminarem, seja por se tratar de tarefa irrealizável em termos práticos, já que é inviável buscar o consenso de cada um dos indivíduos cuja imagem irá compor o banco de dados, seja porque o indivíduo, ante a complexidade e a opacidade do sistema, dificilmente compreenderá para o quê está consentindo exatamente (Fontes *et al.*, 2022).

O paradoxo do consenso é bem explicado por Fontes *et al.* (2022, p. 07, tradução nossa):

> Por um lado, a divulgação completa nas atividades policiais pode ser contraproducente, afetando a eficácia e pertinência da vigilância numa espécie de situação paradoxal em que parece impossível equilibrar a transparência e a eficiência no sentido de justificar o uso de tal tecnologia. Por outro lado, se as pessoas expostas a tais sistemas não estão cientes de que estão sob vigilância, a necessidade de consentir com isso parece redundante.

Não bastasse, a Diretiva da União Europeia para Segurança Pública prevê a desnecessidade de consenso para processamento de dados para fins de segurança pública (Raposo, 2022).

Em termos das tecnologias de reconhecimento facial, portanto, o consenso não é uma saída viável para implementação, nem seria exigível, remanescendo a hipótese de autorização legal (Raposo, 2022).

Portanto, a via para coleta dos dados sensíveis ocorre por meio de autorização legal, o que implica, nos termos da lição de Kriebitz e Lütge (2020), na incidência dos princípios da prevenção de danos e da proporcionalidade. A autorização legal funda-se, então, na prevenção de danos (isto é, no cumprimento eficiente de funções de segurança pública), sem representar, por outro lado, restrição demasiada ao direito individual de proteção de dados, intrinsicamente ligado ao direito à privacidade.

Alguns autores, como Smith e Miller (2022), para lidar com a problemática do consenso, levam a questão para o lado coletivo; ou seja, o consenso não será do indivíduo para coleta das

imagens, mas da sociedade que aceita a coleta e o processamento de imagens faciais em troca de uma coletividade mais segura, o que representa, em essência, a existência de legislação autorizativa do uso – passível, de qualquer forma, de ser contestada a partir do princípio da proporcionalidade, nos termos da lição de Kriebitz e Lütge (2020), uma vez que não se cuida de consenso individual, da pessoa afetada.

Logo, a saída aparenta ser a construção de regulamentação robusta autorizativa da coleta de dados mediante critérios definidos, em que se pondere a finalidade da atividade e seus benefícios com a intromissão nos direitos privados.

Ainda, embora o consenso individual se mostre prescindível, a doutrina especializada discute o direito à informação dos indivíduos acerca do funcionamento do sistema de identificação biométrica à distância em tempo real (Smith e Miller, 2022).

Esse direito à informação também decorreria do estabelecimento de regulamentação prévia e criteriosa acerca do sistema de identificação biométrica à distância em tempo real.

Assim, em síntese, a utilização da mencionada tecnologia implica intromissão no direito à privacidade e no direito à proteção de dados sensíveis, cuja ocorrência será justificada a partir das finalidades adotadas pelo sistema (investigar fatos graves, em que a afetação aos referidos direitos fundamentais e humanos se revele proporcional, no intuito de cumprir também o direito fundamental e humano à segurança pública).

Outros direitos afetados pela utilização de sistema de identificação biométrica à distância em tempo real são os direitos à liberdade de expressão e à reunião.

Como bem coloca a Agência da União Europeia para Direitos Fundamentais, a liberdade de expressão e de informação são pilares da sociedade democrática (FRA, 2020).

O direito à reunião, plasmado, por exemplo, no artigo 5º, XVI, da Constituição Federal (Brasil, 1988), ostenta estreita ligação com a liberdade de expressão e, consequentemente, com o sistema democrático de governo, por possibilitar a participação da população na arena pública mediante reivindicações e expressão de ideias, revelando importante instrumental para controle popular do exercício do poder (Branco, 2013).

Ao se conceber um sistema capaz de detectar a face de qualquer transeunte em via pública, não é difícil perceber as implicações de referido instrumental no exercício dos direitos à liberdade de expressão e à reunião em espaços públicos.

Deveras, ao saberem que estão sendo vigiadas, as pessoas tendem a mudar seu comportamento no espaço público, deixando de agir com a mesma naturalidade, a revelar o potencial efeito resfriador (*chilling effect*) da tecnologia sobre os direitos de liberdade de expressão e de reunião (FRA, 2020).

Como bem colocam Fontes e Perrone (2021, p. 7, tradução nossa), "ferramentas de vigilância conferem poder ao observador", que detém o conhecimento da extensão da vigilância exercida, fato sobre o qual o alvo da vigilância – isto é, o vigiado – carece de conhecimento profundo.

Logo, a utilização de sistemas de identificação biométrica à distância em tempo real, ao possibilitar o monitoramento de uma população inteira em direção a uma vigilância onipresente, ostenta o perigo de banalizar a vigilância em massa, naturalizando mecanismos de vigilância expansiva em caminho progressivo na conversão da emancipação individual e do empoderamento social em restrições incrementais em direitos e autonomia (Fontes e Perrone, 2021; Fontes *et al.* 2022).

Nessa senda, Zalnieriute (2024) aponta que a identificação biométrica à distância em tempo real tem o condão de assemelhar o policiamento em democracias liberais a regimes autoritários, citando exemplo de abordagem de pessoas em razão da participação em protestos.

Em tal contexto, é importante observar o perigo de uso indevido da tecnologia de reconhecimento facial contra determinados grupos específicos, a potencialmente levar a novas discriminações e injustiças (Zalnieriute, 2024).

Aqui relembra-se o conceito de função deformadora (*function creep*), em que, mesmo a confecção da tecnologia para finalidade legítima, pode resvalar para usos indevidos (Selwyn *et al.*, 2024).

A identificação biométrica à distância em tempo real ostenta potencial de afetar o direito a protestar anonimamente, que foi fundamental para expansão de movimentos sociais, eis que os indivíduos devem se sentir confiantes e seguros na possibilidade de reunião em espaços públicos para discordar do *status quo*, sem ficar à mercê de represálias (Zalnieriute, 2024).

Por conta dessas problemáticas, Zalnieriute (2024) sinaliza que diversos acadêmicos, ativistas e políticos opinam pelo banimento da identificação biométrica à distância em tempo real para fins de segurança pública.

É interessante observar, aliás, a existência do caso Glukhin v. Rússia, julgado pela Corte Europeia de Direitos Humanos em 2023 (Lynch, 2024).

O caso revolve a identificação, prisão e persecução de um cidadão russo condutor de protesto solitário e pacífico contra o governo russo no metrô de Moscou (Lynch, 2024). A Corte Europeia considerou o uso do sistema de identificação biométrica altamente intrusivo e violador do direito à liberdade de expressão no caso, sem qualquer aparente questão de segurança pública, quase classificando a tecnologia como inaceitável de maneira geral (Lynch, 2024).

Assim, a identificação biométrica à distância em tempo real apresenta potencial para alterar a natureza do espaço público (Oliveira *et al.*, 2022).

Nessa toada, verifica-se o risco do uso indiscriminado de mencionada tecnologia, pois, ainda que no intuito de segurança pública, ela detém o condão de afetar direitos essenciais à pluralidade social, como de liberdade de expressão e de reunião, intimamente ligados com as bases democráticas da sociedade.

Consequentemente, ao construir sistema de identificação biométrica à distância em tempo real, deve-se ter presente seu efeito deletério para exercício de liberdades individuais e coletivas decorrentes do impacto na percepção individual acerca da ocupação do espaço público. Em tal mister, a fixação de finalidades específicas para atuação do sistema, que não implique monitoramento de pessoas engajadas em atos de liberdade de expressão e direito de reunião, é essencial para que a população não perca senso comunitário do espaço público, evitando, então, risco de arrefecimento no exercício das liberdades democráticas.

Além dessas questões gerais relativas à privacidade e direito de liberdade de expressão e reunião, tendentes a afetar a sociedade como um todo, existem questões particulares atinentes a grupos demográficos.

Como visto, a identificação biométrica à distância em tempo real carrega potenciais vieses decorrentes tanto da menor precisão do algoritmo no reconhecimento de determinados grupos demográficos quanto pela escolha dos locais de posicionamento das câmeras, a focar em determinadas parcelas da população.

Em decorrência, questões de direito antidiscriminatório emergem.

Inclusive, os críticos aos sistemas de identificação biométrica à distância em tempo real apontam o potencial discriminatório como uma das características mais nefastas da tecnologia (Najibi, 2020; Pele e Mulholland, 2023; Santos, 2021).

A Agência da União Europeia para Direitos Fundamentais, ao conceituar discriminação, valeu-se do constante na Directiva 2000/43/CE do Conselho da União Europeia, relativa à aplicação do "princípio da igualdade de tratamento entre as pessoas, sem distinção de origem racial ou étnica", para estabelecer que discriminação ocorre quando "uma pessoa seja objecto de tratamento menos favorável que aquele que é, tenha sido ou possa vir a ser dado a outra pessoa em situação comparável", com base numa característica pessoal real ou imaginada (FRA, 2020).

Em síntese, discriminação consiste na violação ao princípio da igualdade, devido ao tratamento prejudicial ao indivíduo com base em características pessoais sem relevância para a análise em voga, de modo a prejudicá-lo injustificadamente em face de pessoas em situação semelhante.

A contrario sensu, é juridicamente possível o tratamento menos favorável quando isso for direcionado a objetivo legítimo, cujos meios sejam necessários e proporcionais; as fronteiras justificadoras, a seu turno, são muitas vezes definidas caso a caso (FRA, 2020).

O uso de inteligência artificial impõe diversos desafios decorrentes do potencial discriminatório de determinadas tecnologias, conforme exemplos indicados por Bruno Calabrich (citado por Daguer *et al.*, 2022, p. 07):

> Outros casos bastante conhecidos – e reveladores de tratamentos discriminatórios – são os seguintes: (a) o caso do algoritmo de recrutamento da área de recursos humanos da Amazon, que facilitava a contratação de homens em detrimento de mulheres; (b) do algoritmo de categorização de imagens do aplicativo Google Photos, que identificava fotos de pessoas negras como 'gorilas' – sendo digno de nota que a 'solução' da empresa para contornar o problema foi simplesmente bloquear a palavra 'gorila' dos critérios de indexação; e (c) o caso do algoritmo do programa COMPAS (Correctional Offender Management Profiling for Alternative Sanctions), software de auxílio a juízes norte-americanos na avaliação da probabilidade de reincidência para fins de dosimetria da pena, criticado (i) por errar quase duas vezes mais prognósticos de reincidência ao identificar réus negros como futuros criminosos que quando assim identifica réus brancos, e (ii) por errar com muito mais frequência prognósticos de não reincidência ao rotular réus brancos como de baixo risco do que ao rotular réus negros como de baixo risco de reincidência.

No caso da identificação biométrica à distância em tempo real, há, como adiantado, dois potenciais aspectos discriminatórios: a precisão da tecnologia em si, com menor índice de acerto para determinados grupos demográficos, e o possível reflexo de políticas criminais

desproporcionais na implementação da tecnologia, com potencial para exacerbar a discriminação contra determinados grupos, como local de posicionamento das câmeras ou banco de dados que alimentará o algoritmo de inteligência artificial (Lynch, 2024).

Ao se abordar o primeiro ponto acima mencionado, a saber, a falta de precisão do algoritmo em face de determinados grupos demográficos, notadamente de mulheres e pessoas com tons de pele mais escuro, citou-se o celebrado estudo "Gender Shades", em que Buolamwini e Gebru (2018) revelaram, em avaliação de diversos sistemas de identificação facial, maior precisão em homens e em tons de pele clara, de modo que o pior resultado se relacionava à identificação do rosto de mulheres negras.

A menor precisão do algoritmo para tais grupos demográficos é indicada, pela Agência da União Europeia para Direitos Fundamentais, como decorrente da construção de algoritmos fundada na maior representação de homens caucasianos em detrimento de mulheres e indivíduos de origem étnica diversa (FRA, 2020).

Além disso, como já apontado, Wu *et al.* (2023) chegam à conclusão de que diferentes tons de pele dependem de diferentes graus de luminosidade para maior precisão do sistema, de modo que o cenário ideal para as imagens do banco de dados varia de acordo com a tonalidade da pele da pessoa representada.

Isso demonstra que, apesar de melhoras recentes (Lynch, 2024), a falta de precisão dos algoritmos quanto a grupos demográficos deriva em boa medida da construção de tecnologia sem banco de dados de qualidade adequada, isto é, com representatividade da população e com imagens de boa qualidade para todos os grupos demográficos relevantes.

De acordo com Raji *et al.* (2020), a referida questão acaba gerando uma nova tensão entre representatividade e privacidade.

Com efeito, ante a menor precisão dos algoritmos para determinados grupos demográficos, surge a necessidade de maior representação no banco de dados, o que, por outro lado, atrai maior risco de invasão de privacidade das pessoas de tais grupos. Como bem colocam os autores (Raji *et al.*, p. 148-149, tradução nossa):

> Consequentemente, quando se busca conceber paradigma "demograficamente equilibrado", ou seja, um com representação igual dos subgrupos demográficos designados, é mais difícil representar certos grupos em relação a outros. Assim, ao ativamente tentar incluir membros de grupos sub-

> representados, o risco de invasão privacidade aumenta desproporcionalmente para esse grupo.

Logo, ao se buscar consertar o problema da falta de precisão do algoritmo, isso geraria maior risco de invasão de privacidade de grupos minoritários, ante a busca ativa para incremento da representação referida, a desencadear, portanto, em nova problemática a tornar a questão ainda mais complexa.

A questão, portanto, não é simples, na medida em que a busca pela maior precisão do algoritmo em diferentes grupos demográficos também deve respeitar o direito à privacidade, sem vulneração desproporcional, como explorado anteriormente.

Inclusive, ao se tratar de representação, Smith e Mann (2024) também apontam o risco da utilização de banco de dados criminais em que já há sobre-representação de determinados grupos demográficos, o que geraria o potencial de o algoritmo aprender com base nisso e, então, reproduzir vieses contra tal população.

Por esse prisma, a utilização de base de dados exclusivamente criminal poderia ensejar que vieses já presentes no sistema de justiça sejam transportados ao algoritmo, que, como estudado, aprenderá a partir da base de dados fornecida (Smith e Mann, 2024).

Torna-se, então, fundamental relembrar o tratado anteriormente, no sentido de que a tecnologia não é neutra, mas política (Introna e Wood, 2004).

Mesmo que o algoritmo não ostente falhas de precisão em si, a sua utilização pode ocorrer direcionada contra minorias raciais ou em contexto para controlar ou oprimir determinados grupos demográficos (Smith e Mann, 2024).

Nessa senda, deve-se ter em mente que minorias raciais já são submetidas a intervenções desproporcionais pelos sistemas de justiça criminal ao redor do mundo, o que pode ser constatado pela representação exacerbada de determinados grupos demográficos na população carcerária (Smith e Mann, 2024).

Em tal toada, entra em voga o conceito de interseccionalidade, cunhado por Crenshaw, no sentido de que a interrelação de sistemas de poder e opressão gera formas de discriminação qualitativamente diferentes contra indivíduos marginalizados em múltiplas frentes (Raji *et al.*, 2020).

Na identificação biométrica à distância em tempo real, a possibilidade de a utilização da tecnologia carregar vieses exaspera exponencialmente o risco de tratamento discriminatório, na medida em que, se não houver atento controle ao ciclo de vida da inteligência artificial, a aprendizagem do sistema ocorrerá de forma enviesada, gerando, cada vez mais, a consolidação do funcionamento em detrimento de determinados grupos.

Os problemas, então, residem não apenas na tecnologia, mas no próprio sistema de justiça criminal, o que deve ser tratado para poder se cogitar na implementação dos sistemas de identificação biométrica à distância (Smith e Mann, 2024).

Smith e Mann (2024, p. 95, tradução nossa) bem exploram a questão sob os dois aspectos de potencial discriminação do sistema:

> Em vez de proibir totalmente a tecnologia, precisamos nos concentrar na discriminação estrutural e na desigualdade – apelar a uma proibição generalizada de tecnologias, embora possa ser atraente para alguns, não será produtivo a longo prazo, nem é realista. Embora existam aqui questões baseadas em dados que podem ser abordadas, este passo, por si só, não será suficiente, e há necessidade de abordar as questões sociais se quisermos alcançar mudanças significativas. A tecnologia não é o problema, nem é a solução. Em conclusão, há duas perspectivas a se ter em conta: uma perspectiva de dados e uma perspectiva social. Embora estejam inter-relacionadas, precisam ser separadas, a fim de sua interação sociotécnica ser melhor compreendida. Primeiro, podemos ver que, quando a tecnologia é baseada em conjuntos de dados direcionados às populações brancas, ela não funciona com a mesma precisão nas minorias. Em segundo lugar, a tecnologia pode promover o preconceito existente e racismo inerente aos indivíduos e organizações que a implantam e operam, em termos de desigualdade dentro do sistema de justiça criminal e da sociedade mais amplamente. Precisamos garantir que haja representação racial representativa nos conjuntos de dados (a questão técnica) e garantir que não seja utilizado em demasia em áreas onde as minorias estão concentradas (a questão social).

Os autores propõem, então, que, para lidar com o potencial discriminatório da tecnologia, o seu banimento não seria a solução (até porque isso não encerraria os vieses dentro do sistema de justiça criminal); antes deveriam ser implementadas medidas para solução do aspecto técnico (menor precisão do algoritmo em certos grupos demográficos) e do aspecto social (policiamento discriminatório contra determinada parcela da população), com potencial para atacar aspectos estruturantes do racismo e desigualdade no sistema de justiça criminal. A nova tecnologia, nesse contexto, deve se inserir em um movimento consciente da necessidade

de maior igualdade no sistema de justiça criminal e atento ao potencial discriminatório no emprego do sistema caso não haja medidas para detecção e correção de potenciais vieses.

Controles apropriados, como revisões múltiplas, operadores treinados e processos de garantia de qualidade, devem ser garantidos antes de se colocar o sistema em funcionamento, o que é fundamental para confiança do público e utilização do sistema de maneira justa e justificada (Lynch, 2024).

Portanto, durante as diversas etapas de construção e implementação do sistema, devem ser tomadas medidas para evitar vieses em face de determinados grupos a causar discriminações juridicamente vedadas (FRA, 2020).

A tarefa, evidentemente, não é simples, além de ser contínua, durante todo o ciclo de vida da inteligência artificial, em que se deve verificar e corrigir a potencial existência de vieses.

Estabelecida a necessidade de medidas antidiscriminatórias, adentra-se na questão da presunção de inocência em geral.

Como se sabe, a presunção de inocência, plasmada, por exemplo, no artigo 5º, LVII, da Constituição Federal (Brasil, 1988), impõe deveres de conduta das autoridades públicas em relação a abordagem de indivíduos para fins de segurança pública.

Nesse contexto, a abordagem depende de causa provável (*probable cause*) nos termos da doutrina americana (Introna e Nissenbaum, 2010), o que poderia ser traduzido, no ordenamento pátrio, como fundada suspeita exigida pelo artigo 244, *caput*, do Código de Processo Penal (Brasil, 1941):

> A busca pessoal independerá de mandado, no caso de prisão ou quando houver fundada suspeita de que a pessoa esteja na posse de arma proibida ou de objetos ou papéis que constituam corpo de delito, ou quando a medida for determinada no curso de busca domiciliar.

A realização de abordagens sem fundada suspeita (isto é, justa causa) se reveste, em tese, de ilegalidade, conforme demonstram diversos julgados da jurisprudência pátria (a título meramente exemplificativo: AgRg no AREsp n. 2.666.044/SP, relator Ministro Sebastião Reis Júnior, Sexta Turma, julgado em 27/8/2024, DJe de 2/9/2024 – Brasil, 2024).

Por conseguinte, o acionamento automático de forças policiais a partir da correspondência gerada pelo sistema de identificação biométrica à distância em tempo real

poderia representar violação à presunção de inocência, porque a interferência na liberdade e autonomia depende de causa provável (Introna e Nissenbaum, 2010).

Haveria, inclusive, o risco de migrar a presunção de inocência para presunção de culpa em detrimento de indivíduo ainda não julgado, mas reconhecido positivamente pelo sistema de identificação biométrica, a violar o devido processo legal (Selinger e Hartzog, 2019).

Consequentemente, o sistema apenas seria apto a justificar as abordagens ao se considerar que ele preenche o requisito de fundada suspeita presente no artigo 244 do Código de Processo Penal (Brasil, 1941); do contrário, haveria abordagens despidas de justa causa, a violar a presunção de inocência dos cidadãos.

Sobre o ponto, aponta-se que a construção do sistema com robustez técnica e de dados é pré-requisito essencial para que seus resultados sejam confiáveis e possam gerar plausibilidade nas correspondências encontradas, de modo a justificar as abordagens dela decorrentes.

O processo de contínuo monitoramento, revisão e melhoramento durante o ciclo de vida da inteligência artificial (Akbari, 2024) é fundamental para manter a confiabilidade do sistema e, portanto, a robustez dos resultados dele gerados.

Além disso, como tratado anteriormente, o sistema fica sujeito à supervisão humana, de modo que o acionamento das forças de segurança pública não é automático, mas passa pelo crivo de operador humano com conhecimentos técnicos acerca do funcionamento do algoritmo, apto a perceber a ocorrência de falso positivo.

Isso reforça a justa causa para ensejar a abordagem policial a partir da correspondência, pois não apenas a construção do sistema e o monitoramento do seu ciclo de vida devem ocorrer de forma criteriosa a fornecer resultados robustos, como as próprias correspondências positivas devem ser validadas pelo operador humano antes de qualquer ação policial.

Observados esses pontos, as abordagens policiais seriam, inclusive, muito mais objetivas do que aquelas geradas a partir do chamado "tirocínio policial", que ensejam, não raras vezes, ilegalidade da atuação (vide: AgRg no AREsp n. 2.666.044/SP, relator Ministro Sebastião Reis Júnior, Sexta Turma, julgado em 27/8/2024, DJe de 2/9/2024 – Brasil, 2024[10]).

---

10 Veja, por exemplo, o que consta na ementa do referido julgado: "Não houve fundamentação efetivamente concreta a justificar a presença de fundadas suspeitas para a abordagem, tendo a busca pessoal sido realizada, exclusivamente, em decorrência da intuição e impressões subjetivas, intangíveis e não demonstráveis de maneira clara e concreta, apoiadas, por exemplo, exclusivamente, no tirocínio policial (AgRg no RHC n. 160.274/MG,

Nesse sentido, Lynch (2024) destaca que o “olho humano” muitas vezes não é confiável e também é sujeito a vieses, de modo que sistemas de reconhecimento facial são consistentemente mais precisos do que o desempenho humano na identificação de pessoas.

Ademais, não se pode perder de vista que o resultado do sistema não gerará prisões automáticas, mas abordagens para verificação, o que reforça, observados os critérios já mencionados, a sua consonância com o princípio da presunção de inocência.

Outro ponto que emerge da utilização da tecnologia para fins de segurança pública, com possível encarceramento de pessoas, se refere à possibilidade de questionamento do sistema perante Tribunais por parte daquele cuja face foi detectada.

A Agência da União Europeia para Direitos Fundamentais sinaliza a existência do direito à boa administração como um princípio geral do ordenamento europeu, a fim de estabelecer obrigação de a Administração Pública fornecer aos indivíduos afetados as razões do processo decisório, tornando-o transparente e possibilitando que seja contestado pelo interessado (FRA, 2020).

No ordenamento jurídico brasileiro, também há o direito fundamental à boa administração pública (Freitas, 2014),

Desse direito deflui, em tese, o direito de acesso aos dados presentes no sistema e a um remédio efetivo, incidente também na hipótese de identificação biométrica à distância em tempo real, embora com algumas limitações, na medida em que as forças de segurança pública dependem de certa confidencialidade e sigilo para desempenhar trabalho efetivo na persecução criminal (FRA, 2020).

Segundo Matulionyte (2024), transparência e explicabilidade são essenciais para gerar *accountability* do governo no uso de sistemas de reconhecimento facial, permitindo que violações a direitos fundamentais sejam apuradas e punidas.

Tais termos (transparência e explicabilidade), contudo, dependem de aprofundamento sobre sua extensão jurídica (Matulionyte, 2024).

Em linhas gerais, ao haver utilização de inteligência artificial no processo de tomada da Administração Pública, emergem os deveres de transparência e explicabilidade da

---

Ministro Antonio Saldanha Palheiro, Sexta Turma, DJe de 26/4/2023), o que não se revela seguro o suficiente para amparar o decreto condenatório”.

Administração em relação aos cidadãos, fundamental para integridade do processo decisório em ambiente democrático (De Pádua e Lorenzetto, 2024).

Explicablidade poderia ser vista como a quarta lei da robótica[11] e conceituada "como a capacidade de descrever e justificar as decisões tomadas por sistemas de IA, permitindo que sejam entendidas e confiáveis para os humanos" (De Pádua e Lorenzetto, 2024, p. 353). A explicabilidade, em essência, revolve a ideia de que os resultados obtidos pelo sistema de inteligência artificial sejam compreensíveis ao ser humano, no sentido de se entender como os *inputs* colocados no sistema geraram determinado *output* (De Pádua e Lorenzetto, 2024).

Como visto anteriormente, os sistemas de inteligência artificial são opacos por essência, uma vez que a forma de processamento das máquinas para alcançar as inferências, baseadas em modelos matemáticos e algoritmos, seriam incompreensíveis à forma de raciocínio humano (Burrell, 2016). Assim, o princípio da explicabilidade emerge como forma de superar a opacidade, ao se racionalizar o processo decisório da máquina e tornar o resultado obtido pelo sistema compreensível ao ser humano.

A transparência, por sua vez, "permite às pessoas compreenderem como os sistemas de Inteligência Artificial são pesquisados, projetados, implementados e utilizados, levando-se em conta a sensibilidade de cada sistema para vida em sociedade" (De Pádua e Lorenzetto, 2024, p. 357).

Matulionyte (2024) classifica o princípio da transparência como a obrigação de fornecer informações sobre o sistema de inteligência artificial, seu algoritmo e os dados, enquanto a explicabilidade se refere à forma pela qual as decisões da inteligência artificial estão sendo geradas.

Transparência e explicabilidade estão interligados, na medida em que tanto o processo adotado pela Administração Pública quanto o resultado obtido devem ser passíveis de verificação dentro do contexto de aplicação, sendo claros ao cidadão (De Pádua e Lorenzetto, 2024).

Trazendo a temática aos sistemas de reconhecimento facial, Matulionyte (2024) aponta que a explicabilidade variará de acordo com os atores sociais envolvidos. Alguns atores sociais

---

11 As três primeiras leis da robótica seriam: "1) 'um robô não pode ferir um ser humano ou, por inação, permitir que um ser humano venha a ser ferido'; 2) 'um robô deve obedecer às ordens dadas por seres humanos, exceto nos casos em que tais ordens entrem em conflito com a Primeira Lei'; e 3) 'um robô deve proteger sua própria existência, desde que tal proteção não entre em conflito com a Primeira ou com a Segunda Lei' (Asimov, 1950)", citação por De Pádua e Lorenzetto, (2024, p. 356).

deteriam necessidade de obtenção de informações concretas mais detalhadas, como instituições de acreditação, a fim de avaliar os potenciais vieses ou erros do sistema. Segundo a autora, não seriam todos os atores sociais que veriam utilidade na explicabilidade detalhada em razão dos seus dados técnicos, que não seriam compreensíveis ao público geral, como autoridades policiais ou indivíduos afetados (Matulionyte, 2024).

A transparência, por outro lado, é exigível para todos os atores, variando, todavia, em níveis de exigência (Matulionyte, 2024).

Aos indivíduos expostos ao reconhecimento facial e às autoridades policiais não existe necessidade de fornecimento de informação técnica aprofundada do sistema, remanescendo o interesse no conhecimento sobre onde, quando e para qual propósito a tecnologia é utilizada, bem como os níveis de precisão e as balizas legais de utilização, de modo que a exigência de transparência é baixa (Matulionyte, 2024).

Trata-se, basicamente, do direito de ser informado, pré-requisito para o exercício de outros direitos (Raposo, 2022).

Por outro lado, instituições de acreditação e autoridades responsáveis pela auditoria do sistema dependem de alto grau de transparência para realização de avaliação técnica da tecnologia de reconhecimento facial, o que inclui parâmetros do algoritmo, dados de treinamento, processos, métodos, verificação de dados etc. (Matulionyte, 2024).

Um terceiro grupo teria níveis de exigência médio/variáveis de transparência a depender do contexto, como, por exemplo, a autoridade responsável pela aquisição do sistema ou organizações de interesse público, como pesquisadores ou ONGs, em que haverá interesse em dados mais detalhados do sistema a depender do propósito (Matulionyte, 2024).

Esses diferentes níveis de transparência são importantes para determinar, segundo a autora, conflitos com segredo comercial que revolve a tecnologia (Matulionyte, 2024).

Os princípios da transparência e da explicabilidade permitem que os indivíduos sejam informados sobre o funcionamento do sistema de identificação biométrica à distância em tempo real, de modo a possibilitar o uso de remédios efetivos contra eventuais incorreções do sistema (Raposo, 2022).

Conforme a Agência da União Europeia para Direitos Fundamentais, o direito a um remédio efetivo é um direito fundamental que empodera o indivíduo a desafiar qualquer medida que lhe restrinja direitos (FRA, 2020).

Referido direito também incide na identificação biométrica à distância em tempo real, podendo resultar no questionamento do motivo do processamento da imagem facial (FRA, 2020).

Logo, o sistema de identificação biométrica à distância em tempo real deve ostentar níveis de transparência e explicabilidade para permitir que os indivíduos afetados compreendam seu funcionamento e a forma de obtenção do resultado; do contrário, os resultados do sistema tornar-se-ão obscuros e passíveis de questionamento perante os tribunais.

É certo, ainda, que os níveis de transparência e de explicabilidade dependem do interessado e da finalidade da informação pretendida, relembrando-se que determinado grau de confidencialidade e sigilo é necessário para o êxito da atividade policial.

Altos níveis de transparência e explicabilidade devem ser conferidos aos organismos responsáveis por auditar e fiscalizar o sistema de identificação biométrica à distância em tempo real, de modo a garantir que o funcionamento esteja ocorrendo de forma adequada, com robustos níveis de precisão e sem vieses.

Portanto, a transparência e a explicabilidade de forma mais profunda não serão exercidas pelo cidadão em si, que careceria de conhecimentos técnicos para compreensão aprofundada sobre o funcionamento da máquina, mas sim por entidades que exerçam fiscalização contínua do sistema, que estão aptas a exercer escrutínio mais denso sobre as peculiaridades da inteligência artificial, com conhecimentos profundos sobre a matéria.

É fundamental, então, que se constituam organismos idôneos e com representatividade para exercício dessa função, na medida em que funcionarão como representantes da sociedade para garantir o funcionamento adequado do sistema de identificação biométrica à distância em tempo real.

Um último ponto que merece destaque se refere a grupos etários.

A questão inicial diz respeito à precisão do sistema.

As faces de crianças e pessoas idosas são mais suscetíveis aos efeitos do envelhecimento, de modo que a precisão do sistema diminui consideravelmente para tais grupos, mais passíveis a falsos negativos (FRA, 2020).

Assim, ao se tratar a imagem de tais pessoas (e eventuais correspondências obtidas pelo sistema), deve-se ter presente a possibilidade de menor precisão do sistema, sobretudo se a imagem referência do banco de dados é antiga.

Tendo em vista que o sistema operará com supervisão humana como visto anteriormente, a questão será passível de análise do operador humano para identificar potencial erro.

Novamente, então, a supervisão humana se torna elemento-chave para funcionamento adequado do sistema no reconhecimento de grupos sensíveis.

Não bastasse, impõe-se relembrar que crianças e adolescentes são detentores de especial tutela estatal, o que impediria, em tese, o uso de suas imagens para processamento e tratamento pelo banco de dados, salvo em situações excepcionais de segurança pública (Lynch, 2024).

Prepondera, na seara, o melhor interesse da criança, o que reclama cuidados no processamento de imagens faciais de criança devido à sua particular vulnerabilidade (FRA, 2020).

Nada obstante, há casos em que o uso da identificação biométrica à distância em tempo real vem no melhor interesse da criança, o que ocorre, a título de exemplo, quando se trata da localização de crianças desaparecidas, possivelmente vítimas de crimes (FRA, 2020).

Logo, a despeito do cuidado especial que se deve ter em relação às imagens de crianças e adolescentes, não se pode, peremptoriamente, excluir a possibilidade de que suas imagens sejam processadas pelo sistema de identificação biométrica à distância em tempo real, na medida em que isso pode ocorrer exatamente em seu proveito.

Relembra-se, no ponto, o exemplo da ONG americana Thorn, que, mediante emprego de reconhecimento facial, teria conseguido resgatar mais de 10 mil crianças vítimas de tráfico sexual (Oliveira *et al.*, 2022), ou o fato de que a polícia da Índia indiciou que, em 2018, o uso de tecnologia de reconhecimento facial permitiu a identificação de 3000 crianças desaparecidas em somente 4 dias (Zalnieriute, 2024).

Assim, apesar do cuidado especial que se deve ter em relação a grupos etários, notadamente crianças e adolescentes, não seria caso de vedação peremptória do uso da tecnologia para tais grupos.

3.6. PONDERANDO RISCOS COM POTENCIAIS BENEFÍCIOS - POSSÍVEIS SOLUÇÕES

Como se viu nos tópicos anteriores, o uso da identificação biométrica à distância em tempo real, apesar de seu potencial para auxiliar na consecução dos deveres estatais atinentes à segurança pública (que também reflete direito fundamental e humano), apresenta concretos riscos a outros direitos fundamentais e humanos, notadamente de privacidade, direito à reunião, e direito à igualdade, destacando-se, dentre esses pontos, o potencial de exacerbar discriminações no sistema de justiça criminal.

Esse contexto leva a debates sobre a possibilidade e a extensão de uso da referida tecnologia, o que será esmiuçado no presente tópico.

Na doutrina especializada, diante dos impactos a direitos fundamentais e humanos antes delineados, não se encontram autores que defendam a possibilidade de uso irrestrito da tecnologia.

Apesar disso, a prática demonstra que o uso da identificação biométrica à distância em tempo real é realizado, em alguns locais, sem qualquer normativa específica.

Esse, aliás, é o caso do Brasil, em que inexiste normativa específica para uso da tecnologia, e sua implantação gera discussões acerca dos padrões que devem ser adotados para fins de emprego na área da segurança pública (Silva *et al.*, 2022).

Inclusive, dados do Instituto Igarapé de 2019 apontam que, desde 2011, há 48 casos de utilização de tecnologias de reconhecimento facial no Brasil pelo Poder Público ou parceiros privados, com foco primordial nas áreas de transporte e segurança pública (Santos, 2021).

É certo, todavia, que há carência de legislação específica para o uso da tecnologia, sobretudo na área de segurança pública, em que não se aplica a LGPD por força do art. 4º, III, "a" e "d", do referido diploma normativo (Oliveira *et al.*, 2022). Para suprir a lacuna da LGPD, há projetos de lei que tramitam no Congresso Nacional, destacando-se, além da LGPD Penal (Santos, 2021), o Projeto de Lei n. 2338 de 2023 de autoria do Senador Rodrigo Pacheco (PSD/MG).

Inexistindo normatividade específica, incide o que Lynch (2024) chama de autorregulação, em que as entidades responsáveis pela implantação do sistema de identificação biométrica à distância em tempo real assumem o papel de fiscalizar internamente o uso da tecnologia.

Não é difícil antever que tal tipo de encaminhamento enfrenta diversas problemáticas jurídicas.

Em primeiro ponto, Lynch (2024) salienta a falta de legitimidade para realização de autorregulação, na medida em que a decisão sobre o uso da tecnologia depende de debate democrático com envolvimento do público, que é excluído na hipótese de a fiscalização recair somente sobre a própria entidade responsável pelo uso.

Existe, em verdade, cada vez maior preocupação social e de órgãos regulatórios em razão dos potenciais impactos nos indivíduos e na sociedade devido ao uso de identificação biométrica à distância em tempo real sem transparência e legitimidade decorrente de autorização legislativa ou regulatória e sem supervisão (Lynch, 2024).

E a preocupação justifica-se, uma vez que há casos práticos revelando o uso da tecnologia de forma contrária a direitos fundamentais e humanos.

Aqui relembra-se o Caso Glukhin v. Rússia, julgado pela Corte Europeia de Direitos Humanos em 2023, decorrente da identificação, prisão e persecução de um cidadão russo condutor de um protesto solitário e pacífico contra o governo russo no metrô de Moscou (Lynch, 2024). A Corte Europeia considerou o uso do sistema de identificação biométrica altamente intrusivo e violador do direito à liberdade de expressão, sem qualquer aparente questão de segurança pública, parando por pouco em classificar a tecnologia como inaceitável (Lynch, 2024).

Também é interessante salientar o Caso Bridges julgado pela Corte de Apelação do Reino Unido, em que se contestava o uso da identificação biométrica à distância em tempo real pela polícia do País de Gales. Nesse caso, a Corte concluiu pela existência de uma margem de discricionariedade demasiada na forma de emprego da tecnologia, com violação ao direito de privacidade e de expressão das pessoas que queiram protestar (Lynch, 2024).

Os julgados sobre o tema demonstram que o uso irrestrito da identificação biométrica à distância em tempo real, ainda que haja pretensa autorregulação pela entidade responsável pelo uso, incorrem em violações a direitos fundamentais e humanos, sendo inaceitável sob o ponto de vista de um Estado Democrático de Direito.

Ainda, é interessante observar a situação da China, em que há relatos do uso das tecnologias de reconhecimento facial como ferramenta de vigilância em massa destinada ao controle e à repressão, com exemplos como criação de um Sistema de Crédito Social, perseguição de determinados grupos étnicos (Uighur) e supressão de oponentes políticos, mediante emprego da tecnologia para identificação de participantes em protestos (Raposo, 2022).

Os relatos sobre uso irrestrito da identificação biométrica à distância em tempo real na China revelam como a tecnologia pode se converter na faceta autoritária para controle e repressão à população de forma contrária a valores democráticos, sendo incompatível com o quadro de proteção de direitos humanos e fundamentais existentes no Brasil.

Por outro lado, em posição diametralmente oposta à autorregulação ou uso irrestrito, encontra-se o banimento da tecnologia por incompatibilidade com valores democráticos e direitos fundamentais e humanos.

Aliás, em termos práticos, há exemplos do banimento como reação à implementação da tecnologia sem qualquer tipo de regulamentação.

Caso emblemático é da cidade de San Francisco nos Estados Unidos, polo da tecnologia da informação, que, após a implementação da tecnologia em diversas cidades dos Estados Unidos sem qualquer regulamentação (Pereira, 2022), baniu seu uso na referida municipalidade (Fontes e Perrone, 2021).

O uso excessivamente intrusivo da tecnologia na privacidade das pessoas e os possíveis abusos pelas forças de segurança pública levaram San Francisco, juntamente com outras cidades dos Estados Unidos, a banir a tecnologia (FRA, 2020).

O banimento da tecnologia encontra eco em parcela da doutrina, na medida em que se reputa que potenciais benefícios da tecnologia não compensariam os danos causados a direitos e liberdades individuais e coletivas. A título de exemplo, colaciona-se o entendimento de Selinger e Hartzog (2019, p. 122, tradução nossa):

> O resultado final é que, mesmo se os defensores do consentimento e dos requisitos para expedição de mandado [como fundamento para uso da tecnologia] obtiverem tudo em sua lista de desejos, a sociedade ainda acabaria em situação pior. Sofreríamos danos inaceitáveis à nossa autonomia coletiva através de uma série de botões de anuência e mandados de busca e apreensão fornecidos pelo governo, com a sede insaciável da indústria por mais acesso às nossas vidas. Há apenas uma maneira de acabar com os danos da vigilância facial. Banindo-a.

Pontos que sustentam tal posicionamento também revolvem a suposta baixa efetividade do sistema em realmente auxiliar a prevenção e repressão de crimes e o potencial discriminatório (Santos, 2021).

Alguns autores apontam a falta de estudos para se concluir sobre o impacto da tecnologia nas investigações criminais, seu nível de precisão e confiabilidade (Dushi, 2020).

Estudos relativos ao emprego da tecnologia no Reino Unido, onde o tema ainda carece de regulamentação específica, sugerem que as tecnologias seriam discriminatórias e careceriam de eficiência (Khan e Rizvi, 2021).

Nessa linha, a Professora de Direito da Universidade da Califórnia Veena Dubal (2019) argumenta o acerto da cidade de San Franscisco em banir da tecnologia, devido à falta de precisão e, sobretudo, ao viés racial e político na vigilância estatal.

Nesse sentido, argumenta-se (Dubal, 2019, p. 02, tradução nossa):

> Mesmo que a vigilância facial seja 100% neutra e desprovida de tendências discriminatórias, os seres humanos determinarão quando e onde ocorre a vigilância. Os seres humanos – com vieses implícitos e explícitos – tomarão decisões discricionárias sobre como utilizar os dados coletados. E os seres humanos — muitas vezes os mais vulneráveis — serão os afetados de forma desproporcional e injusta.

Nada obstante as pertinentes críticas ao sistema, entende-se que o banimento de tecnologia capaz de melhor proteger a sociedade e prevenir crimes não é a solução ideal (Dushi, 2020). Por isso, Dushi (2020) reputa que, em vez de uso irrestrito ou o banimento, deve haver regulamentação detalhada que não deixa espaço para lacunas interpretativas a serem abusadas por empresas ou pelo governo para controlar os cidadãos, mas isso ainda dependeria, na visão da autoria, de estudos mais aprofundados sobre a eficácia do sistema na área de segurança pública.

As críticas apontadas para banimento do sistema se inserem numa discussão mais ampla de desigualdade do sistema de justiça criminal (Najibi, 2020). Em geral, os defensores do banimento visualizam a tecnologia como potencial exacerbador de discriminação do sistema de justiça criminal e, por isso, concluem pelo seu banimento.

Acontece que, mesmo com o banimento, remanesceriam as questões discriminatórias do sistema de justiça criminal que são apontadas como problemáticas; como salientam Smith e Mann (2024), a solução não seria o banimento da tecnologia, que ostenta potencial no cumprimento do dever estatal de segurança pública (direito fundamental e humano da população), mas a adoção de medidas para solução do aspecto técnico (maior precisão do

algoritmo em diversos grupos demográficos) e do aspecto social (policiamento discriminatório contra determinada parcela da população), com enfrentamento de aspectos estruturantes do racismo e da desigualdade no sistema de justiça criminal.

Em semelhante toada, encontra-se o entendimento de Daguer *et al.* (2022, p. 09-10):

> O reconhecimento facial é um importante instrumento na segurança pública e receberá cada vez maior espaço na esfera estatal e também na seara penal. Todavia, entende-se que a tecnologia deve ser empregada com cautela, tendo em vista a necessidade de aprimoramento legal do instituto no tocante aos limites na relação com direitos fundamentais, a fim de se evitar medidas discriminatórias em desfavor dos cidadãos e ofensa aos direitos fundamentais dos indivíduos.

Semelhante conclusão é alcançada pela Agência da União Europeia para Direitos Fundamentais, considerando que o uso da identificação biométrica à distância em tempo real é possível em situações excepcionais (FRA, 2020).

Inclusive, o banimento peremptório, sem qualquer possibilidade de uso, não se mostraria ideal por impedir a evolução tecnológica e a concretização de instrumental com potencial profícuo à segurança pública. Nesse sentido, a lição de Magalhães e Gomes (2021, p. 178), em que se elogia a iniciativa de regulação europeia:

> Internacionalmente, tem-se adotado iniciativas pela regulamentação, tanto no sentido de proibição geral, como ocorre em cidades e estados estadunidenses, quanto em vias de proibição condicionada a alguns usos. Deve-se observar, no entanto, que a proibição irrestrita desestimula a evolução dessas tecnologias e sua possível aplicação no combate a preconceitos, de forma que é uma opção com muitas limitações.
>
> O projeto de lei proposto pela Comissão Europeia ao Parlamento Europeu, dentre os aqui analisados, foi o que apresentou melhores soluções sobre o uso de tecnologias de reconhecimento facial para fins de segurança pública e, logo, pode contribuir como referência na discussão normativa no contexto brasileiro. As limitações propostas permitem que o desenvolvimento tecnológico e aperfeiçoamento dessas tecnologias não seja interrompido, assim como oferecem medidas rigorosas de controle e uso responsável.

Logo, adentra-se nessa terceira proposta de solução, consistente na regulação da tecnologia, com fixação de balizas para seu uso.

A regulação do uso da identificação biométrica à distância em tempo real aparece como alternativa a permitir o uso da tecnologia em consonância com a proteção de direitos fundamentais e humanos, equilibrando, a um só tempo, os ganhos do sistema para efetividade na consecução da atividade de segurança pública – dever estatal e direito fundamental e humano da população – com os potenciais riscos do sistema.

Veja-se, nesse sentido, a lição de Mobilio (2022, p. 23, tradução nossa):

> Argumentamos que é possível regular as tecnologias de reconhecimento facial de uma forma que equilibre os benefícios deste poder de vigilância com a proteção dos direitos fundamentais, a preservação da ordem democrática e do Estado de direito.

A regulação, todavia, é complexa, uma vez que os ganhos não podem significar violações a direitos fundamentais e humanos desproporcionais, a impor arranjo fino e extremamente equilibrado para uso do sistema.

O tema é exposto por Daguer *et al.* (2022, p. 09):

> Embora seja inevitável o aumento das máquinas de reconhecimento facial, é necessária forte regulação em face da questão da utilização tendo em vista que adotam decisões automatizadas. Ademais, no campo da segurança pública e da investigação criminal, é necessário ter ainda mais rigor, 'a fim de que seus detentores e executores sejam responsabilizados diante de um sistema que possa ser usado contra os indivíduos e de possível instrumentalização para perseguição e de criminalização, em atuação desviada da prevista em lei'.

A regulação criteriosa e rigorosa do sistema vem a ser a solução dos conflitos de direito que giram em torno da identificação biométrica à distância em tempo real.

Relembrando o Caso Bridges, a Corte de Apelação entendeu ser de suma importância que as agências de segurança pública utilizem ao máximo as tecnologias disponíveis para cumprimento do seu mister, contanto isso ocorra dentro de parâmetros legais aceitáveis (Pereira, 2022).

Não se trata de vedar peremptoriamente o uso da identificação biométrica à distância em tempo real, mas adequá-la a um cenário que, a um só tempo, busque maior eficácia na

promoção da segurança pública, sem implicar, por outro lado, em violações descabidas de direitos fundamentais e humanos.

Para fins de regulamentação, Lynch e Campbell (2024) apontam três possibilidades: legislação doméstica, fixação de princípios e guias estatais, fixação de parâmetros internacionais.

Para edição legislação doméstica sobre o reconhecimento facial e tecnologias biométricas, as autoras citam estudo da Comissão Australiana de Direitos Humanos que sinalizou os seguintes pontos a serem observados: proteção a direitos humanos, aplicação baseada em risco, suporte para *compliance*, transparência no uso das tecnologias de reconhecimento facial, regulação e supervisão efetivas, responsabilidade e reparação, compatibilidade jurisdicional (Lynch e Campbell, 2024).

Sobre a compatibilidade jurisdicional, é pertinente notar a necessidade de "desenvolvimento tecnológico autóctone, adequado à cultura do país, que poderia mitigar falhas oriundas de diferenciais demográficos geradores de vieses nos algoritmos empregados" (Olivera *et al.*, 2022, p. 127).

A fixação de princípios e guias estatais incide na ausência de legislação específica, valendo-se de premissas gerais para aplicação de inteligência artificial (Lynch e Campbell, 2024). Essa solução parece ser insuficiente para possibilitar o uso de identificação biométrica à distância em tempo real, que, pelos riscos e alto grau de intrusão, depende de legislação robusta e detalhada, como já salientado.

Por fim, a fixação de normativa internacional é o que ocorre, por exemplo, com o Regulamento Europeu da Inteligência Artificial, estudado no presente trabalho.

Cuida-se de importante mecanismo a conferir efeito extraterritorial e influenciar as legislações nacionais (Lynch e Campbell, 2024).

Ainda, qualquer que seja a forma adotada, depende-se da criação de órgão regulador robusto, na medida em que o ciclo de vida da inteligência artificial deve ser monitorado de forma contínua (Lynch e Campbell, 2024).

Fontes e Perrone (2021), para definição da medida proporcional do uso na segurança pública, apontam que deve ser primeiro determinado se os benefícios superam os riscos, considerando, inclusive, outras soluções possíveis, e, ainda que positivo o resultado dessa ponderação, deve-se avaliar o impacto político e social da tecnologia, ante a concessão de poder

de vigilância às autoridades públicas mediante acesso a dados biométricos sensíveis da população.

Assim, a regulamentação não pode perder de vista a necessidade de proteção de dados ligados ao direito de privacidade (Dushi, 2020).

Segundo Dushi (2020), a política regulatória da identificação biométrica à distância em tempo real deve observar os seguintes critérios: uso de acordo com o ordenamento jurídico, legitimidade, necessidade e proporcionalidade, privacidade e proteção de dados pessoais, não discriminação.

Raposo (2022), por sua vez, detalha uma proposta de regulamentação.

Inicialmente, deve-se vedar o uso da identificação biométrica à distância em tempo real para uso não relacionado à segurança pública, dado o grau de intrusão da tecnologia na privacidade das pessoas (Raposo, 2022). Inclusive, deve-se buscar evitar a possibilidade de usos velados que desdobrem para situações abusivas; é dizer, por trás do pretexto de proteção da segurança pública, pode haver intenção de vigilância em massa, o que deve ser vedado (Raposo, 2022).

A autora pontua, em tal senda, que a vigilância em massa por sua própria natureza já configura violação a direitos fundamentais, especialmente de privacidade e proteção de dados pessoais (Raposo, 2022).

Fixadas as hipóteses de uso da tecnologia, deve haver avaliação se a finalidade perseguida é legítima, como ocorre com qualquer tecnologia cujos impactos afetem direitos fundamentais (Raposo, 2022). Assim, a tecnologia deve ser utilizada para finalidade legítima e relevante à ordem jurídica.

Em seguida, adequadas as hipóteses e finalidades de uso, impõe-se realizar teste de proporcionalidade da tecnologia, por meio dos subprincípios da adequação, necessidade e proporcionalidade em sentido estrito (Raposo, 2022).

Em tal cenário, demonstra-se que a finalidade de processamento de dados sensíveis não pode ser alcançada por meios menos intrusivos em direitos fundamentais (Raposo, 2022). Outrossim, a tecnologia não deve resultar em intromissão demasiada em direitos fundamentais, em que os benefícios não superam os prejuízos causados (Raposo, 2022).

Nessa senda, a identificação biométrica à distância em tempo real será reservada aos casos estritamente necessários, direcionados a crimes graves, observando, ainda, a necessidade

de proteção de grupos vulneráveis (Raposo, 2022). O alvo deve ser somente a pessoa de interesse, salvo se, por razões justificadas, for imposto pela investigação criminal uma base mais abrangente (Raposo, 2022).

A legislação deve, ademais, estabelecer parâmetros para captação das imagens e período de retenção (Raposo, 2022).

Além disso, há o direito de as pessoas serem informadas sobre a utilização da identificação biométrica à distância em tempo real, o que é pré-requisito ao exercício de outros direitos, como de um remédio efetivo (Raposo, 2022). Como bem pontuam Fontes e Perrone (2021), a transparência é essencial.

Deve haver distinção entre o direito à informação anterior e posterior, já que, em muitos casos, o direito só poderá ser exercido de forma posterior, sob pena de, ocorrendo anteriormente, prejudicar a eficiência do sistema (Raposo, 2022).

Mecanismos de *compliance* são essenciais, dependendo de transparência e escrutínio público, de modo que deve haver responsabilidade das autoridades públicas pela identificação biométrica à distância em tempo real, com possibilidade de insurgência dos indivíduos em face do uso da tecnologia (Raposo, 2022).

Dentro, ainda, da ideia de monitoramento do sistema, devem ser fixados mecanismos para garantir a precisão do sistema, destacando-se que falsos positivos são extremamente danosos em se tratando de tecnologia empregada para segurança pública, o que é ainda mais sensível diante da possibilidade de dano sistemático a minorias étnicas (Raposo, 2022).

Ainda, deve haver supervisão humana do funcionamento da inteligência artificial, uma vez que decisões automáticas pela máquina devem ser banidas (Raposo, 2022).

Adotadas essas medidas, a autora considera possível a criação de paradigma legal capaz de excluir o risco de vigilância extensiva, em consonância com quadro normativo atento à proteção de direitos fundamentais e humanos (Raposo, 2022).

Sintetizando essas questões, a Agência da União Europeia para Direitos Fundamentais, ponderando benefícios e riscos, sinalizou que a identificação biométrica à distância em tempo real deve ser relegada a situações excepcionais, limitadas ao combate de terrorismo e outras formas de crimes sérios, bem como para encontrar pessoas desaparecidas e vítimas de crimes (FRA, 2020).

O Regulamento Europeu da Inteligência Artificial, em linhas gerais, observou tais apontamentos e previu robustos parâmetros para aplicação da identificação biométrica à distância em tempo real (Lynch, 2024).

Estabelecidas as considerações teóricas acerca da tecnologia, adentra-se na solução dada pelo referido Regulamento, no intuito de avaliar sua compatibilidade com a proteção de direitos fundamentais e humanos e se seria alternativa possível ao cenário brasileiro.

4. IDENTIFICAÇÃO BIOMÉTRICA À DISTÂNCIA EM TEMPO REAL NO REGULAMENTO EUROPEU

Como normativa regulatória, o Regulamento Europeu da Inteligência Artificial (União Europeia, 2024)[12] desponta como talvez um dos primeiros diplomas em âmbito mundial a dissecar a identificação biométrica à distância em tempo real e permitir sua utilização na segurança pública em situações excepcionalíssimas e de forma altamente condicionada.

Seja pela profundidade legislativa, seja pela influência exercida em outros ordenamentos (efeito Bruxelas), o Regulamento Europeu se destaca como marco regulatório a merecer atenção, sobretudo ante o caso brasileiro, em que impera vácuo normativo específico sobre a matéria.

Aliás, até pelo prisma histórico, percebe-se a grande influência das normativas europeias no direito penal e processual penal brasileiro.

Sobre o tema, ao assinalar a evolução histórica do direito penal, Prado, Carvalho e Carvalho (2015) evidenciam a forte influência europeia na normatização nacional, além de assentar que "o Direito Penal comum é resultado da fusão do Direito romano, do Direito germânico, do Direito canônico e dos direitos nacionais, com a prevalência do primeiro, especialmente após o Século XII, por obra dos práticos" (Prado, Carvalho e Carvalho, 2015, p. 85).

Os autores revelam que a origem do pensamento jurídico nacional parte da Europa, destacando, nesse contexto, as principais escolas do pensamento penal, a saber, a escola clássica, a escola positiva, a escola moderna alemã, a escola técnico-jurídica, a escola correcionalista e o movimento de defesa social (Prado, Carvalho e Carvalho, 2015).

Inclusive, as teorias da conduta, alicerce do Direito Penal, são calcadas basicamente no pensamento europeu, de origem notadamente germânica (Brandão, 2000).

Na mesma senda, ao analisar as teorias relevantes ao processo penal brasileiro, Lopes Jr. (2013) indica a forte influência europeia para formação do pensamento acadêmico pátrio.

---

12 UNIÃO EUROPEIA. **Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho,** de 13 de junho de 2024 que cria regras harmonizadas em matéria de inteligência artificial e que altera os Regulamentos (CE) n.o 300/2008, (UE) n.o 167/2013, (UE) n.o 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e as Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (**Regulamento da Inteligência Artificial**).

Percebe-se, então, a enorme influência do pensamento europeu na formação da doutrina nacional, tratando-se de tradição cuja origem é bem anterior ao próprio fenômeno chamado de efeito Bruxelas.

Portanto, o estudo do Regulamento Europeu da Inteligência Artificial também se faz relevante em razão da tradição brasileira em endossar o pensamento europeu.

Consignado tal ponto, antes de adentrar nas especificidades da regulação conferida pelo Regulamento para o uso da identificação biométrica à distância em tempo real, é prudente compreender características gerais do referido Diploma, que se insere no âmbito transnacional e, portanto, não é idêntico a uma legislação doméstica.

4.1. PANORAMA E HISTÓRICO DE ELABORAÇÃO DO REGULAMENTO

O Tratado de Roma, instituidor da Comunidade Econômica Europeia (CEE), de 1957, já previu a criação de um mercado comum regional, o que, todavia, representava tarefa complexa, dependente de uma regulação harmonizada dos produtos a impedir discriminações entre os Estados-Membros em razão das origens dos produtos (Frankel e Galland, 2015).

A construção de arcabouço normativo a compreender a estrutura de tais regras harmonizadas dependeu de esforços contínuos, atualmente representadas pelo selo "CE" (*Conformité Européenne*), indicativo de que determinado produto segue as regras harmonizadas europeias para transitar nos mercados internos do bloco (Frankel e Galland, 2015).

A harmonização é atualmente baseada no chamado "Novo Quadro Legislativo", seguido também pelo Regulamento Europeu da Inteligência Artificial (Ortigosa, 2024).

O Novo Quadro Legislativo foi adotado em 2008, resultante do Regulamento (CE) n.º 765/2008 e da Decisão n.º 768/2008/CE, instrumentos normativos do Parlamento Europeu e do Conselho da União Europeia, destinados a melhorar o funcionamento do mercado interno e fortalecer as condições de colocação no mercado de produtos, mediante aperfeiçoamento de regras de proteção de consumidores em face de produtos perigosos, melhoramento da qualidade da avaliação de conformidade por meio de critérios claros e regras de acreditação, e clarificação do símbolo "CE" (Vicheva e Mitova, 2018).

Segundo INMETRO (2020, p. 06), em estudo feito sobre a padronização europeia, a Nova Abordagem é "feita com base nos chamados requisitos essenciais, e que estes requisitos

essenciais são genéricos e aplicáveis a grandes categorias de produtos". Os requisitos essenciais direcionam-se a questões de segurança ou outros interesses coletivos cuja tutela interessa aos Estados (INMETRO, 2020).

A definição de requisito essencial se encontra no Guia Azul de 2016 sobre a Aplicação das Regras da UE em matéria de Produtos: "Os requisitos essenciais definem os resultados a alcançar ou os riscos a tratar, mas não especificam as soluções técnicas para o fazer" (União Europeia, 2016, p. 39).

O processo para obtenção do selo "CE" sob a ótica do Novo Quadro Legislativo pode ser representado pela figura abaixo:

Figura 7 – Harmonização da legislação técnica por meio do Novo Quadro Legislativo

Fonte: Extraído de Vicheva e Mitova, (2018, p. 301).

Esse procedimento consiste no seguinte: os requisitos essenciais são elementos obrigatórios a serem cumpridos pelos produtos para obtenção do selo de conformidade ("CE"); as normas harmonizadas, por sua vez, refletem o detalhamento técnico dos requisitos essenciais e são confeccionados por órgãos de padronização, mas não são obrigatórias (diferente dos requisitos essenciais, portanto), embora o seu preenchimento gere presunção de conformidade (ou seja, o fornecedor do produto pode comprovar o cumprimento dos requisitos essenciais por outra forma que não o preenchimento das normas harmonizadas, porém, em tal hipótese, o ônus recai sobre ele); o preenchimento dos requisitos essenciais, por fim, é feito por meio de uma avaliação de conformidade (Vicheva e Mitova, 2018).

As normas harmonizadas são fixadas por organismos europeus mediante solicitação da Comissão Europeia, conforme INMETRO (2020, p. 07):

> [...] há então uma clara complementaridade entre a regulamentação técnica que utiliza o conceito de requisitos essenciais, ou seja, as Diretivas Nova

> Abordagem, e as normas técnicas voluntárias (as Normas Harmonizadas) que os traduzem em requisitos técnicos.

Embora não sejam obrigatórios, os padrões harmonizados trazem diversos benefícios, como retirar inconsistências técnicas por disparidade de regulamentação entre países, consolidação de confiança nas trocas, aumento da competitividade entre empresas, garantia de segurança e saúde dos consumidores etc. (Vicheva e Mitova, 2018).

O Guia Azul de 2016 sobre a Aplicação das Regras da UE em Matéria de Produto bem elucida o ponto (União Europeia, 2016, p. 42):

> As normas harmonizadas nunca substituem os requisitos essenciais juridicamente vinculativos. Uma especificação apresentada numa norma harmonizada não constitui uma alternativa a um requisito essencial pertinente ou a outro requisito legal, mas apenas um eventual meio técnico para lhe dar cumprimento. Na legislação de harmonização relativa aos riscos, tal significa, em particular, que um fabricante, mesmo quando utiliza normas harmonizadas, continua a ser plenamente responsável pela avaliação de todos os riscos do seu produto a fim de determinar quais os requisitos essenciais (ou outros) aplicáveis. Após essa avaliação, o fabricante pode optar, em seguida, por aplicar as especificações contidas nas normas harmonizadas a fim de aplicar «medidas de redução dos riscos» (166) especificadas nas normas harmonizadas. Na legislação de harmonização relativa aos riscos, as normas harmonizadas proporcionam frequentemente determinados meios que permitem reduzir ou eliminar os riscos, embora os fabricantes continuem a ser plenamente responsáveis pela avaliação dos mesmos, a fim de identificar os riscos em causa, e pela identificação dos requisitos essenciais aplicáveis, a fim de selecionar as normas harmonizadas ou outras especificações adequadas.

Desse excerto, percebe-se outro ponto relevante do Novo Quadro Legislativo, no sentido de que, mesmo cumprindo os requisitos essenciais, o fabricante não deixa de ser responsável pela contínua avaliação dos riscos, no intuito de sempre garantir a segurança do seu produto.

Sobre a avaliação de conformidade, ela é realizada por órgãos acreditados pelas Autoridades Nacionais de cada Estado-Membro (Frankel e Galland, 2015). Cada Estado-Membro instituirá uma autoridade pública responsável por acreditar (conferir legitimidade) às instituições responsáveis pela avaliação de conformidade destinada ao preenchimento dos requisitos essenciais e, portanto, adequação aos padrões europeus (tal avaliação pode ser por meio do cumprimento dos padrões harmonizados, o que gera presunção de conformidade – ou

mediante demonstração do preenchimento dos requisitos essenciais por outros meios, hipótese cujo ônus recai sobre o interessado).

Conforme o Guia Azul de 2016 sobre a Aplicação das Regras da UE em Matéria de Produto (União Europeia, 2016, p. 88):

> A acreditação é a atestação por um organismo nacional de acreditação com base nas normas harmonizadas de que um organismo de avaliação da conformidade tem a competência técnica para exercer uma atividade específica de avaliação da conformidade.

Outro ponto fundamental recai sobre a vigilância de mercado a ser exercida pelo Estado-Membro, no intuito de impedir a circulação de produtos não conformes (Vicheva e Mitova, 2018).

Destaca-se que tal fiscalização exercida por cada Estado obedece a legislação doméstica, não havendo processos harmonizados nesse ponto, já que se trata de uma atividade decorrente da "organização do Estado, da sua administração e do próprio ordenamento jurídico" (INMETRO, 2020, p. 39).

Nos termos do Guia Azul de 2016 sobre a Aplicação das Regras da UE em Matéria de Produto (União Europeia, 2016, p. 98):

> A fiscalização do mercado garante aos cidadãos um nível de proteção equivalente em todo o mercado único, independentemente da origem do produto. Além disso, a fiscalização do mercado é importante para os interesses dos operadores económicos, na medida em que contribui para a eliminação da concorrência desleal.

A incumbência da fiscalização do mercado recai sobre os Estados-Membros, inclusive para garantir o cumprimento da legislação da União Europeia (União Europeia, 2016).

É pertinente pontuar, ainda, que, para complementar o Novo Quadro Legislativo, editou-se, em 2019, o Regulamento (UE) 2019/1020 sobre vigilância de mercado e conformidade de produtos

O Regulamento Europeu da Inteligência Artificial segue esse arcabouço normativo (Ortigosa, 2024).

Assim, o Regulamento Europeu da Inteligência Artificial vai observar os cinco pilares aqui destacados: requisitos essenciais, normas harmonizadas, avaliação de conformidade, responsabilidade (dos fornecedores) e vigilância de mercado.

O estudo prévio desse arcabouço é importante para compreender o sentido dos requisitos essenciais fixados no Regulamento, cujo cumprimento pode ocorrer pela observância das normas harmonizadas ou por outros meios a ônus do interessado, até porque se trata de estrutura normativa que, pela sua índole transnacional, não se confunde com uma normativa doméstica, que tende a ser mais detalhada.

Feita essa introdução para contextualização do ato normativo, aborda-se o histórico da elaboração do Regulamento Europeu da Inteligência Artificial.

Como visto em tópicos anteriores, a inteligência artificial se revela sistema autônomo, complexo e opaco, cujo funcionamento é imprevisível, de modo que existem riscos associados à tecnologia, que, também, por sua vez, apresenta potenciais de inovação sem precedentes, com capacidade para resolver problemas nas mais diversas áreas.

Ante a possibilidade de lesão a direitos fundamentais pelo uso indiscriminado de inteligência artificial, preocupação foi levantada sobre a questão em âmbito europeu (Madiega, 2024).

Em 2019, foram publicados os seguintes textos pelo Grupo Independente de Peritos de Alto Nível sobre a Inteligência Artificial criado pela Comissão Europeia em junho de 2018: Orientações Éticas para uma IA de Confiança e Recomendações de Políticas e Investimentos para IA Confiável (Madiega, 2024).

São textos com recomendações voltadas a uma abordagem da inteligência artificial centrada no ser humano, caracterizados como *soft-law*, pela falta de coercibilidade (Madiega, 2024).

Diante da importância do tema e da sua expansão, a Comissão Europeia, após a edição das recomendações, inclinou-se para disciplina normativa da questão, mediante adoção de regras harmonizadas a possibilitar a circulação de sistemas de inteligência artificial na União Europeia (Madiega, 2024).

Logo, a mera previsão de recomendações, sem caráter coercitivo, na visão da Comissão Europeia, seria insuficiente a regular e conter os riscos associados ao uso de inteligência

artificial, motivo pelo qual o órgão pendeu para elaboração de legislação regulatória sob o prisma do Novo Quadro Legislativo.

Em tal contexto, a Comissão Europeia realizou uma consulta pública e publicou uma avaliação de impacto relativa à regulação da IA, um estudo correlato e um rascunho de proposta legislativa; disso foram encontradas cinco características específicas da inteligência artificial que clamavam pela existência de regulação: (i) opacidade (limitada capacidade de a mente humana compreender o funcionamento de sistemas de IA), (ii) complexidade (iii) adaptação contínua e imprevisibilidade (iv) comportamento autônomo e (v) dependência de dados e da qualidade dos dados (Madiega, 2024).

Assim, em 21 de abril de 2021, a Comissão Europeia apresentou proposta de regulação da inteligência artificial. A cronologia do processo legislativo do Regulamento é bem descrita pelo sítio eletrônico da União Europeia dedicado ao ato (EU Artificial Intelligence Act, 2024).

Sobre o aspecto cronológico da elaboração do ato, alguns pontos relevantes merecem ser citados.

Em 06 de agosto de 2021, estudo analítico do uso de biometria sob perspectivas éticas e legais realizado por Departamento do Parlamento Europeu é publicado (EU Artificial Intelligence Act, 2024).

Durante o trâmite do ato legislativo, sobrevieram as inteligências artificiais generativas e de finalidade geral, o que acarretou na inclusão de tais modelos na proposta legislativa (EU Artificial Intelligence Act, 2024), cujo foco inicial era a abordagem de risco, baseada na atividade desempenhada pelo sistema (o que não funciona propriamente, quando a tecnologia não apresenta um propósito predefinido).

Assim, em 13 de maio de 2022, o Presidente do Conselho publica proposta para regular GPAI (Inteligência Artificial de Uso Geral), sistemas de IA capazes de realizar uma ampla gama de tarefas (EU Artificial Intelligence Act, 2024).

Em 09 de dezembro de 2023, o Parlamento e o Conselho, durante as negociações interinstitucionais (trílogos), atingem um acordo provisório sobre o regulamento, momento em que é divulgado amplamente na mídia sobre a adoção do Regulamento, embora formalmente o ato dependesse de alguns trâmites legislativos (EU Artificial Intelligence Act, 2024).

Em 13 de março de 2024, o regulamento, acordado nas negociações com os Estados-Membros em dezembro de 2023, foi formalmente aprovado no Parlamento pelos eurodeputados

por 523 votos a favor, 46 votos contra e 49 abstenções. Já em 21 de maio de 2024, o Conselho Europeu formalmente adotou o Regulamento (EU Artificial Intelligence Act, 2024).

Em 12 de julho de 2024, o Regulamento é publicado no Diário Oficial da União Europeia, de modo que é, a partir de tal data, que o ato está oficialmente em vigência na União Europeia, apesar de haver *vacatio legis* para determinados pontos (EU Artificial Intelligence Act, 2024).

Assim, no presente momento, o processo legislativo já foi concluído, e o Regulamento integra o ordenamento jurídico europeu. Especificamente quanto à identificação biométrica à distância em tempo real, a normativa, nos termos do art. 113, que fixa a *vacatio legis*, passa a valer a partir de 02 de fevereiro de 2025 (União Europeia, 2024).

4.2. CONCEITOS GERAIS DO REGULAMENTO

O Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho de 13 de junho de 2024 cria regras harmonizadas em matéria de inteligência artificial e que altera os Regulamentos (CE) n.o 300/2008, (UE) n.o 167/2013, (UE) n.o 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e as Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828, sendo denominado Regulamento da Inteligência Artificial, conforme versão em português do texto (União Europeia, 2024).

Sobre o diploma, é interessante observar que ele conta com um preâmbulo de 44 páginas composto por 180 itens explicativos e fundantes da regulação realizada (União Europeia, 2024).

Desse preâmbulo é possível extrair diversas lições para compreensão do texto legal, pertinentes, inclusive, para sanar eventuais dúvidas acerca da aplicação do Regulamento.

Um primeiro ponto que merece destaque – e que vai guiar toda a interpretação a ser feita das disposições do Regulamento – diz respeito ao item 6 do preâmbulo, que prevê que a inteligência artificial deve ser concebida como uma tecnologia antropocêntrica, isto é, centrada no ser humano, cujo objetivo final é aumentar o bem-estar humano (União Europeia, 2024).

Logo, a inteligência artificial não é um fim em si própria, mas instrumento em prol do ser humano.

Nesse contexto, a necessidade de regulação emerge do potencial inovador atrelado a riscos aos seres humanos em razão do uso da tecnologia. Essa dualidade é bem exposta pelos itens 4 e 5 do preâmbulo (União Europeia, 2024, p. 2).:

> (4) A IA é uma família de tecnologias em rápida evolução que contribui para um vasto conjunto de benefícios económicos, ambientais e sociais em todo o leque de indústrias e atividades sociais. Ao melhorar as previsões, otimizar as operações e a repartição de recursos e personalizar as soluções digitais disponibilizadas às pessoas e às organizações, a utilização da IA pode conferir importantes vantagens competitivas às empresas e contribuir para progressos sociais e ambientais, por exemplo, nos cuidados de saúde, na agricultura, na segurança alimentar, na educação e na formação, nos meios de comunicação social, no desporto, na cultura, na gestão das infraestruturas, na energia, nos transportes e na logística, nos serviços públicos, na segurança, na justiça, na eficiência energética e dos recursos, na monitorização ambiental, na preservação e recuperação da biodiversidade e dos ecossistemas e na atenuação das alterações climáticas e adaptação às mesmas.
>
> (5) Ao mesmo tempo, em função das circunstâncias relativas à sua aplicação, utilização e nível de evolução tecnológica específicos, a IA pode criar riscos e prejudicar interesses públicos e direitos fundamentais protegidos pela legislação da União. Esses prejuízos podem ser materiais ou imateriais, incluindo danos físicos, psicológicos, sociais ou económicos.

O risco, nos termos do art. 3º, item 2, do Regulamento, conceitua-se como a "combinação da probabilidade de ocorrência de danos com a gravidade desses danos" (União Europeia, 2024, p. 46). Portanto, dois fatores influenciam a avaliação de risco: a chance de sua ocorrência e a gravidade do risco caso ocorra.

Para alicerçar referida regulação, são estipulados, no item 27 do preâmbulo, 7 princípios, a saber: 1) iniciativa e supervisão por humanos; 2) solidez técnica e segurança; 3) privacidade e governação dos dados; 4) transparência; 5) diversidade, não discriminação e equidade; 6) bem-estar social e ambiental e 7) responsabilização (União Europeia, 2024).

Diversos desses princípios já foram abordados nesse trabalho de alguma forma.

Sem prejuízo, cumpre conceituá-los, ainda que de forma sucinta.

A iniciativa e supervisão humana indica que a operação da inteligência artificial estará sempre sujeita ao ser humano, reforçando o axioma de que se trata de tecnologia antropocêntrica, que não deve operar por si própria (União Europeia, 2024).

Solidez e segurança relacionam-se a robustez do sistema em enfrentar problemas, diminuindo chances de danos não intencionais, bem como a resiliência em face de medidas voltadas a alterar seu desempenho e para utilização ilícita por terceiros (União Europeia, 2024).

Privacidade e governação de dados referem-se à proteção de dados inerente aos bancos que são montados para construção da base de conhecimento do sistema, que devem, ainda, observar a qualidade e a integridade (União Europeia, 2024).

Transparência impõe rastreabilidade e explicabilidade ao sistema de inteligência artificial, conferindo direito de informação às pessoas afetadas (União Europeia, 2024).

Diversidade, não discriminação e equidade significam que a tecnologia deve ser promovida de forma não resultar em desigualdades, privilegiando igualdade de acesso e de gênero, bem como a diversidade cultural (União Europeia, 2024).

Bem-estar social e ambiental reflete o viés sustentável a ser incorporado nos sistemas de inteligência artificial, que devem ter em mente os impactos a longo prazo nas pessoas, na sociedade e na democracia (União Europeia, 2024).

Responsabilização, por fim, indica que o beneficiário da tecnologia deve responder pelos danos causados por esta, tendo em conta que o comportamento imprevisível e autônomo do sistema, por ser fato atrelado à sua própria natureza, não exonera tal responsabilidade (União Europeia, 2024).

Além disso, não se pode esquecer que o Regulamento se encontra inserido dentro do Novo Quadro Legislativo, de modo que ele segue as premissas de 1) Requisitos Essenciais; 2) Normas Harmonizadas; 3) Avaliação de Conformidade; 4) Responsabilidade; e 5) Vigilância de Mercado.

Para fins de conceituação de sistema de inteligência artificial, o que, como visto anteriormente, é um problema e gera debates doutrinário, o Regulamento adotou o seguinte conceito em seu artigo 3º, item 1 (União Europeia, 2024, p. 46):

> «Sistema de IA», um sistema baseado em máquinas concebido para funcionar com níveis de autonomia variáveis, e que pode apresentar capacidade de adaptação após a implantação e que, para objetivos explícitos ou implícitos, e com base nos dados de entrada que recebe, infere a forma de gerar resultados, tais como previsões, conteúdos, recomendações ou decisões que podem influenciar ambientes físicos ou virtuais.

Do que se extrai da redação legal, verifica-se que a característica fundamental do sistema de inteligência artificial é a capacidade de inferir baseada em máquinas (Madiega, 2024).

Tal conceito está alinha ao exposto no presente trabalho, embora, aqui, tenha se adentrado no potencial de solução autônoma e no melhoramento contínuo decorrente da capacidade de aprendizado dependente de dados.

O conceito do Regulamento foi criticado por apresentar suposta vagueza, o que geraria incerteza jurídica (Madiega, 2024).

Tais críticas, contudo, foram respondidas pelo próprio Regulamento, que, no item 12 do preâmbulo, explica a motivação para adoção de mencionado conceito nos seguintes termos (União Europeia, 2024, p. 4):

> O conceito de «sistema de IA» constante do presente regulamento deverá ser definido de forma inequívoca e estar estreitamente alinhado com o trabalho das organizações internacionais ativas no domínio da IA, a fim de assegurar a segurança jurídica, facilitar a convergência internacional e a ampla aceitação, concedendo em simultâneo a flexibilidade suficiente para se adaptar a rápidas evoluções tecnológicas neste domínio. Além disso, a definição deverá basear-se nas principais características dos sistemas de IA que o distinguem de sistemas de software ou abordagens de programação tradicionais mais simples e não deverá abranger sistemas baseados nas regras definidas exclusivamente por pessoas singulares para executarem operações automaticamente. Uma característica principal dos sistemas de IA é a sua capacidade de fazer inferências. Esta capacidade de fazer inferências refere-se ao processo de obtenção dos resultados, tais como previsões, conteúdos, recomendações ou decisões, que possam influenciar ambientes físicos e virtuais, e à capacidade dos sistemas de IA para obter modelos ou algoritmos, ou ambos, a partir de entradas ou dados. As técnicas que permitem fazer inferências durante a construção de um sistema de IA incluem abordagens de aprendizagem automática que aprendem com os dados a forma de alcançarem determinados objetivos, e abordagens baseadas na lógica e no conhecimento que fazem inferências a partir do conhecimento codificado ou da representação simbólica da tarefa a resolver. A capacidade de um sistema de IA fazer inferências vai além do tratamento básico de dados, permitindo a aprendizagem, o raciocínio ou a modelização. O termo «baseado em máquinas» refere-se ao facto de os sistemas de IA funcionarem em máquinas. A referência a objetivos explícitos ou implícitos visa sublinhar que os sistemas de IA podem funcionar de acordo com objetivos explícitos definidos ou com objetivos implícitos. Os objetivos do sistema de IA podem ser diferentes da finalidade prevista para o sistema de IA num contexto específico. Para efeitos do presente regulamento, deverá entender-se por «ambientes» os contextos em que os sistemas de IA operam, ao passo que os resultados gerados pelo sistema de IA refletem diferentes funções desempenhadas pelos sistemas de IA e incluem previsões, conteúdos, recomendações ou decisões. Os sistemas de IA são concebidos para operar com diferentes níveis de autonomia, o que significa que têm um certo grau de independência das ações efetuadas por intervenção humana e de capacidade

> para funcionarem sem intervenção humana. A capacidade de adaptação que um sistema de IA poderá apresentar após a implantação refere-se a capacidades de autoaprendizagem, permitindo que o sistema mude enquanto estiver a ser utilizado. Os sistemas de IA podem ser utilizados autonomamente ou como componentes de um produto, independentemente de o sistema estar fisicamente incorporado no produto (integrado) ou servir a funcionalidade do produto sem estar incorporado nele (não integrado).

Percebe-se que, ao sinalizar que o conceito está "estreitamente alinhado com o trabalho das organizações internacionais ativas no domínio da IA", o Regulamento indica o rigor teórico da definição dada, que, ademais, não poderia ser muito rígida, sob pena de carecer de "flexibilidade suficiente para se adaptar a rápidas evoluções tecnológicas neste domínio" (União Europeia, 2024, p. 4).

Na referida explicação, constata-se que a característica principal é, exatamente, a capacidade de inferência, a qual engloba o processo de aprendizagem.

Entende-se que, para fins legais, a conceituação está, ao que tudo indica, adequada para as finalidades que se pretende, não sendo rígida demais a deixar brechas legais para alguns sistemas escaparem da regulamentação, conferindo maleabilidade ao intérprete.

O âmbito de aplicação do Regulamento é definido pelo seu artigo 2º e pode ser resumido nos seguintes pontos: sistemas de IA utilizados na União Europeia, independentemente da localização do desenvolvedor; implantadores de sistema de IA localizados na EU; e desenvolvedores ou implantadores localizados fora da UE, mas cujo produto do sistema de IA é utilizado na IA (União Europeia, 2024).

É importante observar que o Regulamento é inaplicável para áreas fora do escopo da UE ou para atividades militares, relacionadas a defesa e segurança nacional, e de índole exclusivamente de pesquisa e desenvolvimento científico (União Europeia, 2024).

Essa observação é de extrema importância ao presente trabalho, na medida em que as considerações tecidas no tópico sobre o uso da identificação biométrica à distância em tempo real não incidem caso a tecnologia seja direcionada a atividades militares, de defesa ou de segurança nacional.

Isso deixa relevantes áreas fora da regulamentação, sobretudo da identificação biométrica à distância em tempo real que perpassa, muitas vezes, por questões de segurança nacional ou defesa, além de relegar certa margem de discricionariedade aos Estados na classificação da finalidade da tecnologia, a potencializar eventuais burlas do Regulamento.

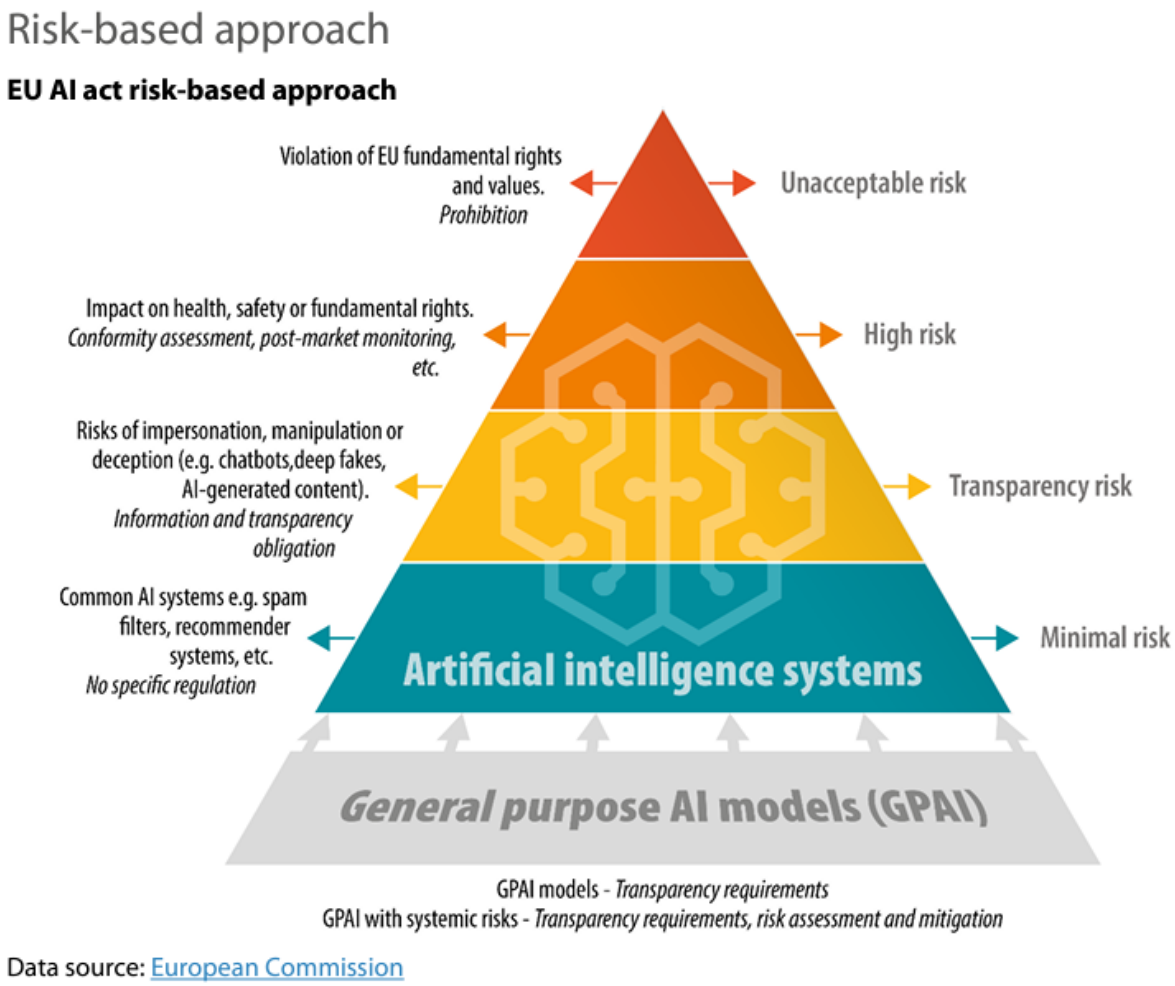
Isso porque muitas vezes a linha entre atividades de segurança pública rotineiras e segurança nacional é tênue, o que abre margem para buscar se escapar da incidência da estrita regulação do mencionado diploma.

Assim, ao serem lidas as disposições do Regulamento sobre identificação biométrica à distância em tempo real, deve-se ter em mente que elas não são aplicáveis para atividades militares, de defesa ou de segurança nacional, áreas em que ainda vige, a rigor, vácuo normativo no âmbito da regulação internacional da União Europeia.

A atualização de conceitos do Regulamento, por sua vez, é realizada pela Comissão Europeia por meio de atos de execução e atos delegados, o que permite que o Regulamento permaneça adequado ante a evolução tecnológica (União Europeia, 2024).

Último ponto a ser destacado sobre o Regulamento, em linhas gerais, é que ele adota Abordagem Baseada em Risco (*Risk-Based Approach*), divididos em cinco categorias: Inaceitáveis (proibidos); Alto Risco (impactos na segurança das pessoas ou direitos fundamentais); Risco Limitado (obrigações de transparência); Mínimo Risco (adesão facultativa a códigos de conduta); GPAI (Inteligência Artificial de Finalidade Geral – riscos sistêmicos). Referida abordagem é bem sintetizada pela imagem abaixo:

Figura 8 – Abordagem Baseada em Risco



Fonte: Extraído de Madiega (2024, p. 07).

A finalidade do sistema é que definirá o risco, salvo no caso das inteligências artificiais de finalidade geral, em que não há propósito pré-definido, mas podem desempenhar ampla gama de tarefas distintas, de modo que a avaliação de risco é realizada a partir da capacidade de processamento, bem como por decisão da Comissão Europeia.

A partir da figura acima, percebe-se que, a depender do grau de risco, haverá diferentes padrões regulatórios.

Os riscos proibidos são, evidentemente, vedados, de modo que a sua implantação ou comercialização gera responsabilização e enseja a tomada de medidas pela autoridade nacional responsável pela fiscalização do mercado.

Os sistemas de risco elevados possuem condicionantes para funcionar. Dentre as obrigações, podem ser destacados os seguintes pontos: Implementação de gestão de risco

(artigo 9º); Governança de dados (artigo 10); Elaboração de documentação técnica (artigo 11); Manutenção de registros (artigo 12); Transparência e informação pelos desenvolvedores aos implantadores (artigo 13); Supervisão humana (artigo 14); Exatidão, solidez e cibersegurança (artigo 15) (União Europeia, 2024).

Ainda, eles são submetidos à avaliação de conformidade para recebimento da marca "CE" (artigo 48) (União Europeia, 2024).

São sistemas de alto risco, conforme artigo 6º do Regulamento: 1) aquele em que o sistema de IA é utilizado como componente de segurança de um produto (ou é o próprio produto), constante na legislação harmonizada prevista no Anexo I, sendo que a legislação determina que referido produto passe por avaliação de conformidade perante um terceiro; ou 2) aquele incluído no Anexo III (União Europeia, 2024).

O anexo III lista, resumidamente, as seguintes atividades para as quais o uso de IA representará alto risco: Dados biométricos; Infraestrutura crítica; Educação e formação profissional; Emprego, gestão de trabalhadores e acesso ao emprego por conta própria; Serviços essenciais públicos ou privados; Aplicação da lei; Migração, asilo e controle de fronteira; Administração da Justiça e processos democráticos (União Europeia, 2024).

Esses sistemas listados no anexo III devem realizar avaliação de impacto em direitos fundamentais como previsto no artigo 27, o que reflete, em essência, um verdadeiro teste de ponderação para verificar se o uso da inteligência artificial se mostra adequado, necessário e proporcional em sentido estrito para as finalidades visadas à vista dos direitos impactados (União Europeia, 2024).

Consigna-se, ainda, que, conforme item 3 do artigo 6º, um sistema do anexo III não será considerado de alto risco se ele "não representar um risco significativo de danos para a saúde, a segurança ou os direitos fundamentais das pessoas singulares, nomeadamente se não influenciarem de forma significativa o resultado da tomada de decisões" (União Europeia, 2024, p. 54).

Lendo-se referido dispositivo *a contrario sensu*, percebe-se que os sistemas de risco elevado revolvem "risco significativo de danos para a saúde, a segurança ou os direitos fundamentais das pessoas singulares".

Portanto, o fundamento da regulamentação de tais sistemas reside nos mencionados riscos.

Dito isso, verifica-se, então, que o uso de inteligência artificial para segurança pública, em regra geral, cai na modalidade de alto risco (pois englobada a atividade de segurança pública no anexo III), sujeitando-se às condicionantes inerentes a tal uso.

Entretanto, como será visto a seguir, a identificação biométrica à distância em tempo real detém regras próprias.

Feito esse panorama geral do Regulamento, cumpre, então, adentrar propriamente no tema do presente trabalho, a identificação biométrica à distância em tempo real.

4.3. DISPOSIÇÃO GERAL SOBRE IDENTIFICAÇÃO BIOMÉTRICA

O artigo 3º do diploma traz definições dos conceitos adotados pelo Regulamento. Conforme visto no tópico anterior, por exemplo, é em referido artigo que consta a definição do termo sistema de inteligência artificial (União Europeia, 2024).

Aqui serão apontadas as definições pertinentes para o objeto de estudo.

Em primeiro lugar, o item 34 do referido artigo conceitua dado biométrico como “dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos” (União Europeia, 2024, p. 48).

Esse conceito está de acordo com o estudado anteriormente, no sentido de que os dados biométricos se referem a características do indivíduo e são sensíveis na medida em que permitem a individualização da pessoa.

Nos itens 35 e 36, também na esteira da doutrina acima mencionada, o Regulamento diferencia a identificação biométrica da verificação biométrica (União Europeia, 2024).

Segundo analisado, a identificação biométrica envolve o processo de comparação da face de uma pessoa com uma multidão, enquanto a verificação consiste na comparação individual.

O Regulamento estabelece exatamente essa diferenciação, ao assinalar que a identificação biométrica implica reconhecimento automatizado de uma pessoa a partir da comparação de dados biométricos capturados com os constantes em uma base de dados, ao passo que a verificação revolve comparação um para um (União Europeia, 2024).

No item 41 do referido artigo 3º, o Regulamento classifica os sistemas de identificação biométrica à distância como aqueles para "identificar pessoas singulares, sem a sua participação ativa, normalmente à distância, por meio da comparação dos dados biométricos de uma pessoa com os dados biométricos contidos numa base de dados de referência" (União Europeia, 2024, p. 48).

É interessante notar que a identificação biométrica não necessariamente se limita ao uso da face, mas pode englobar, conforme item 35, "características humanas físicas, fisiológicas, comportamentais ou psicológicas para efeitos de determinação da identidade de uma pessoa singular" (União Europeia, 2024, p. 48).

O presente estudo, por sua vez, limitou-se à identificação pela face por se tratar da forma mais corriqueira e desenvolvida de utilização de tal tecnologia; certamente usos para identificação por meio de características corporais diversas ou comportamentais dependeriam de aprofundamento específico sobre o tema, além de maior desenvolvimento da própria tecnologia, que, no tópico, ainda é assaz incipiente.

Avançando, ao conceituar "Sistema de identificação biométrica à distância em tempo real", que é propriamente o objeto do presente estudo, o Regulamento, no artigo 3º, item 42, disciplina que é o sistema de identificação biométrica à distância cuja comparação e identificação acontecem sem atraso significativo, de modo a enquadrar o conceito não apenas na identificação instantânea, mas a englobar também sistemas cuja operação aconteça com ligeiro atraso (União Europeia, 2024).

Essa previsão de ligeiro atraso, como explicado pelo próprio artigo 3º, item 42, ocorre para evitar eventuais burlas às regras que disciplinam o "Sistema de identificação biométrica à distância em tempo real", impedindo, portanto, alegações de que atrasos não expressivos retirariam a natureza de "tempo real" do sistema (União Europeia, 2024).

Se o sistema não opera, efetivamente, em tempo real, isto é, se realmente conta com atrasos significativos nos processos de comparação e identificação, então ele é classificado como "sistema de identificação biométrica à distância em diferido", cujo conceito está no item 43 do artigo 3º (União Europeia, 2024).

Portanto, ao tratar da identificação biométrica à distância em tempo real, o Regulamento Europeu, em leitura dos itens 34, 35, 41 e 42 do preâmbulo, traz disciplina sobre o: "sistema de IA concebido para identificar pessoas singulares, sem a sua participação ativa, normalmente à distância, por meio da comparação dos dados biométricos de uma pessoa com os dados

biométricos contidos numa base de dados de referência", cujo processamento ocorre "sem atraso significativo" (União Europeia, 2024, p. 48).

Cuida-se exatamente do objeto do presente estudo.

A explicação para adoção de mencionados conceitos consta no item 17 do preâmbulo do referido Diploma (União Europeia, 2024, p. 05):

> O conceito de «sistema de identificação biométrica à distância» a que se refere o presente regulamento deverá ser definido, de modo funcional, como um sistema de IA que se destina à identificação de pessoas singulares sem a sua participação ativa, normalmente à distância, por meio da comparação dos dados biométricos de uma pessoa com os dados biométricos contidos numa base de dados de referência, independentemente da tecnologia, dos processos ou dos tipos de dados biométricos específicos utilizados. Tais sistemas de identificação biométrica à distância são geralmente utilizados para detetar várias pessoas ou o seu comportamento em simultâneo, a fim de facilitar significativamente a identificação de pessoas singulares sem a sua participação ativa. Estão excluídos os sistemas de IA concebidos para serem utilizados na verificação biométrica, que inclui a autenticação, cujo único objetivo seja confirmar que uma pessoa singular específica é quem afirma ser e confirmar a identidade de uma pessoa singular com o único objetivo de lhe conceder acesso a um serviço, desbloquear um dispositivo ou ter acesso de segurança a um local. Essa exclusão justifica-se pelo facto de esses sistemas serem suscetíveis de ter um impacto ligeiro nos direitos fundamentais das pessoas singulares em comparação com os sistemas de identificação biométrica à distância que podem ser utilizados para o tratamento de dados biométricos de um grande número de pessoas sem a sua participação ativa. No caso dos sistemas «em tempo real», a recolha dos dados biométricos, a comparação e a identificação ocorrem de forma instantânea, quase instantânea ou, em todo o caso, sem um desfasamento significativo. Não deverá haver, a este respeito, margem para contornar as regras do presente regulamento sobre a utilização «em tempo real» dos sistemas de IA em causa prevendo ligeiros desfasamentos no sistema. Os sistemas «em tempo real» implicam a utilização «ao vivo» ou «quase ao vivo» de materiais, como imagens vídeo, gerados por uma câmara ou outro dispositivo com uma funcionalidade semelhante. No caso dos sistemas «em diferido», ao invés, os dados biométricos já foram recolhidos e a comparação e a identificação ocorrem com um desfasamento significativo. Estes sistemas utilizam materiais, tais como imagens ou vídeos, gerados por câmaras de televisão em circuito fechado ou dispositivos privados antes de o sistema ser utilizado relativamente às pessoas singulares em causa.

Tais definições, então, decorrem da necessidade de tratamento específico da identificação biométrica à distância em tempo real pelo seu alto impacto em direitos fundamentais e humanos, como salientado no presente trabalho.

A utilização de sistemas de identificação biométrica à distância em tempo real na segurança pública, é regulada, por sua vez, pelo artigo 5º do Regulamento (União Europeia, 2024).

Mencionado dispositivo disciplina as práticas de inteligência artificial proibidas.

Em regra, pelo artigo, 5º, alínea *h*, assenta-se a vedação do uso em espaços públicos[13] de sistemas de identificação biométrica à distância em tempo real para aplicação da lei (União Europeia, 2024).

O termo aplicação da lei refere-se à tradução em português do termo *law enforcement*, cuja definição se encontra no artigo 3º, item 46, no seguinte sentido (União Europeia, 2024, p. 49):

> «Aplicação da lei», as atividades realizadas por autoridades responsáveis pela aplicação da lei ou em nome destas para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, incluindo a proteção contra ameaças à segurança pública e a prevenção das mesmas.

Trata-se, então, das atividades revolvendo segurança pública.

Consequentemente, a utilização de identificação biométrica à distância em tempo real para fins de segurança pública é, por via de regra, vedada pelo Regulamento Europeu.

As razões para tal vedação são explicadas no preâmbulo do mencionado Diploma normativo.

No item 32 do preâmbulo, estabelece-se que referida tecnologia é (União Europeia, 2024, p. 09):

> [...] particularmente intrusiva para os direitos e as liberdades das pessoas em causa, visto que pode afetar a vida privada de uma grande parte da população, dar origem a uma sensação de vigilância constante e dissuadir indiretamente o exercício da liberdade de reunião e de outros direitos fundamentais.

---

13 Isto é: "qualquer espaço físico, público ou privado, acessível a um número indeterminado de pessoas singulares, independentemente da eventual aplicação de condições de acesso específicas e independentemente das eventuais restrições de capacidade", conforme artigo 3º, item 44, do Regulamento (União Europeia, 2024, p. 48).

Além disso, também se assenta a potencialidade de resultados enviesados e efeitos discriminatórios pelo uso da tecnologia, com especial relevância para idade, etnia, raça, sexo ou deficiência (União Europeia, 2024).

Prosseguindo, o item 32 assinala que esses potenciais riscos são exacerbados quando a tecnologia é utilizada em tempo real, ou seja, sem atrasos significativos, pela limitação de controle decorrente da contingência temporal (União Europeia, 2024).

Por conta desses fatores, o item 33 do preâmbulo justifica a proibição da identificação biométrica à distância em tempo real (União Europeia, 2024).

Relembra-se que o conceito de risco se refere à "combinação da probabilidade de ocorrência de danos com a gravidade desses danos"; em tal toada, considerou-se que a identificação biométrica à distância em tempo real para fins de segurança pública ocasiona probabilidade de danos consideráveis a direitos fundamentais e humanos de modo a justificar o banimento da tecnologia em regra (União Europeia, 2024).

É interessante pontuar que, conforme artigo 5º, alínea *h*, a vedação direciona-se à aplicação da lei, ou seja, à segurança pública, de modo que outras finalidades no uso da tecnologia recairão na disciplina geral de tratamento de dados biométricos previstas no artigo 9º do Regulamento da União Europeia 2016/679, que se trata do Regulamento Geral sobre a Proteção de Dados (União Europeia, 2024).

Segundo o artigo 9º Regulamento Geral sobre a Proteção de Dados, é vedado o tratamento de dados pessoais sensíveis, salvo se o titular tiver fornecido consentimento expresso, o dado for público, ou o tratamento for realizado nas finalidades previstas no item 2 do mencionado artigo, que incluem proteção de interesses do próprio titular do dado, interesse público importante entre outros.

Sobre esses usos diversos, o item 39 do preâmbulo dispõe que (União Europeia, 2024, p. 11):

> Para outros fins que não a aplicação da lei, o artigo 9.o, n.o 1, do Regulamento (UE) 2016/679 e o artigo 10.o, n.o 1, do Regulamento (UE) 2018/1725 proíbem o tratamento de dados biométricos, salvo nos casos abrangidos pelas exceções limitadas previstas nesses artigos. Em aplicação do artigo 9.o, n.o 1, do Regulamento (UE) 2016/679, a utilização da identificação biométrica à

> distância para outros fins que não a aplicação da lei já foi objeto de decisões de proibição por parte das autoridades nacionais de proteção de dados.

Logo, a vedação de uso é expressamente direcionada para segurança pública no Regulamento da Inteligência Artificial, embora outras finalidades já tenham o uso vedado no âmbito da RGPD por decisões das autoridades nacionais de proteção de dados[14].

O item 59 do preâmbulo indica que as utilizações de inteligência artificial para fins de segurança pública são "caracterizadas por um grau substancial de desequilíbrio de poder e podem conduzir à vigilância, detenção ou privação da liberdade de uma pessoa singular, bem como ter outras repercussões negativas nos direitos fundamentais" (União Europeia, 2024, p. 17).

Assim, em razão dessa assimetria de poder, previu-se vedação específica para a identificação biométrica à distância em tempo real na segurança pública.

Nada obstante, em exercício de ponderação legislativa, o próprio Regulamento excepcionou possibilidades de uso da tecnologia para segurança pública, de modo que determinados doutrinadores, como Mobilio (2023), sequer consideram que houve proibição propriamente dita.

Sob o ponto de vista do presente trabalho, considera-se adequada a permissão de uso da tecnologia de maneira rigorosa e em casos restritos, sujeita a mecanismos de controle e monitoramento, porquanto se cuida de mecanismos com potenciais benefícios a incrementar a atividade de segurança pública em prol da coletividade.

4.4. HIPÓTESES EXCEPCIONAIS DE POSSIBILIDADE PARA SEGURANÇA PÚBLICA

O item 33 do preâmbulo, mencionado anteriormente, aponta que, apesar de a regra geral ser a vedação, é possível a utilização de identificação biométrica à distância em tempo real em "situações enunciadas exaustivamente e definidas de modo restrito, em que essa utilização é

14 Torna-se fundamental relembrar, aqui, que tanto o Regulamento da Inteligência Artificial quanto a RGPD se inserem no Novo Quadro Legislativo, em que a fiscalização de mercado é exercida por autoridades nacionais.

estritamente necessária por motivos de interesse público importante e cuja importância prevalece sobre os riscos" (União Europeia, 2024, p. 09).

A própria alínea *h* do artigo 5º já contém, em seu texto, as hipóteses excepcionais para uso da identificação biométrica à distância em tempo real na segurança pública.

Permite-se o uso, desde que estritamente necessário, para os seguintes fins (União Europeia, 2024, p. 52):

> i) busca seletiva de vítimas específicas de rapto, tráfico de seres humanos ou exploração sexual de seres humanos, bem como a busca por pessoas desaparecidas,
>
> ii) prevenção de uma ameaça específica, substancial e iminente à vida ou à segurança física de pessoas singulares ou de uma ameaça real e atual ou real e previsível de um ataque terrorista,
>
> iii) a localização ou identificação de uma pessoa suspeita de ter cometido uma infração penal, para efeitos da realização de uma investigação criminal, ou instauração de ação penal ou execução de uma sanção penal por alguma das infrações referidas no anexo II e puníveis no Estado-Membro em causa com pena ou medida de segurança privativa de liberdade de duração máxima não inferior a quatro anos.

Adentrando em cada uma das hipóteses para deferimentos, é possível tecer as seguintes considerações.

A primeira hipótese refere-se à localização de vítimas ou de pessoas desaparecidas.

O Regulamento limita, quanto às vítimas, os crimes suspeitos, a saber, rapto, tráfico de seres humanos e exploração sexual (União Europeia, 2024).

Para compreender a incidência típica, será analisado o Código Penal Português (Decreto-Lei n.º 48/95), eis que se trata de Regulamento incidente na União Europeia, e a versão analisada reflete a tradução portuguesa do Diploma.

Pois bem, o crime de rapto está tipificado no artigo 161 do Código Penal Português nos seguintes termos (Portugal, 1995, art. 161, capítulo IV, título I, livro II):

> 1 - Quem, por meio de violência, ameaça ou astúcia, raptar outra pessoa com a intenção de:
>
> a) Submeter a vítima a extorsão;

> b) Cometer crime contra a liberdade e autodeterminação sexual da vítima;
>
> c) Obter resgate ou recompensa; ou
>
> d) Constranger a autoridade pública ou um terceiro a uma acção ou omissão, ou a suportar uma actividade;
>
> é punido com pena de prisão de 2 a 8 anos.
>
> 2 - Se no caso se verificarem as situações previstas:
>
> a) No n.º 2 do artigo 158.º, o agente é punido com pena de prisão de 3 a 15 anos;
>
> b) No n.º 3 do artigo 158.º, o agente é punido com pena de prisão de 8 a 16 anos.
>
> 3 - Se o agente renunciar voluntariamente à sua pretensão e libertar a vítima, ou se esforçar seriamente por o conseguir, a pena pode ser especialmente atenuada.

Ao que se percebe, referido tipo penal não encontra perfeita correspondência no ordenamento brasileiro. Ele seria uma conjunção entre os artigos 148, §1º, V (sequestro e cárcere privado para fins libidinosos) e 159 (extorsão mediante sequestro) do Código Penal Brasileiro (Brasil, 1940).

O crime de tráfico de seres humanos está previsto como tráfico de pessoas no artigo 160 do Código Penal Português (Portugal, 1995, art. 160, capítulo IV, título I, livro II):

> 1 - Quem oferecer, entregar, recrutar, aliciar, aceitar, transportar, alojar ou acolher pessoa para fins de exploração, incluindo a exploração sexual, a exploração do trabalho, a mendicidade, a escravidão, a extração de órgãos ou a exploração de outras atividades criminosas:
>
> a) Por meio de violência, rapto ou ameaça grave;
>
> b) Através de ardil ou manobra fraudulenta;
>
> c) Com abuso de autoridade resultante de uma relação de dependência hierárquica, económica, de trabalho ou familiar;
>
> d) Aproveitando-se de incapacidade psíquica ou de situação de especial vulnerabilidade da vítima ou
>
> e) Mediante a obtenção do consentimento da pessoa que tem o controlo sobre a vítima;
>
> é punido com pena de prisão de três a dez anos.

> 2 - A mesma pena é aplicada a quem, por qualquer meio, recrutar, aliciar, transportar, proceder ao alojamento ou acolhimento de menor, ou o entregar, oferecer ou aceitar, para fins de exploração, incluindo a exploração sexual, a exploração do trabalho, a mendicidade, a escravidão, a extração de órgãos, a adoção ou a exploração de outras atividades criminosas.
>
> 3 - No caso previsto no número anterior, se o agente utilizar qualquer dos meios previstos nas alíneas do n.º 1 ou actuar profissionalmente ou com intenção lucrativa, é punido com pena de prisão de três a doze anos.
>
> 4 - As penas previstas nos números anteriores são agravadas de um terço, nos seus limites mínimo e máximo, se a conduta neles referida:
>
> a) Tiver colocado em perigo a vida da vítima;
>
> b) Tiver sido cometida com especial violência ou tenha causado à vítima danos particularmente graves;
>
> c) Tiver sido cometida por um funcionário no exercício das suas funções;
>
> d) Tiver sido cometida no quadro de uma associação criminosa; ou
>
> e) Tiver como resultado o suicídio da vítima.
>
> 5 - Quem, mediante pagamento ou outra contrapartida, oferecer, entregar, solicitar ou aceitar menor, ou obtiver ou prestar consentimento na sua adopção, é punido com pena de prisão de um a cinco anos.
>
> 6 - Quem, tendo conhecimento da prática de crime previsto nos n.os 1 e 2, utilizar os serviços ou órgãos da vítima é punido com pena de prisão de um a cinco anos, se pena mais grave lhe não couber por força de outra disposição legal.
>
> 7 - Quem retiver, ocultar, danificar ou destruir documentos de identificação ou de viagem de pessoa vítima de crime previsto nos n.os 1 e 2 é punido com pena de prisão até três anos, se pena mais grave lhe não couber por força de outra disposição legal.
>
> 8 - O consentimento da vítima dos crimes previstos nos números anteriores não exclui em caso algum a ilicitude do facto.

Referido tipo penal guarda estreita correlação com o artigo 149-A do Código Penal Brasileiro, que tipifica, igualmente, o tráfico de pessoas (Brasil, 1940).

Sobre a tipificação brasileira, é interessante observar que ela foi incluída pela Lei n. 13.344/2016, que também incluiu os artigos 13-A e 13-B no Código de Processo Penal Brasileiro (Brasil, 1941).

O artigo 13-A do Código de Processo Penal Brasileiro permite a requisição por membro do Ministério Público ou pelo Delegado de Polícia de dados e informações cadastrais da vítima

ou de suspeitos nos crimes de sequestro e cárcere privado, redução à condição análoga à de escravo, tráfico de pessoas, sequestro relâmpago (artigo 158, §3º, do Código Penal) e extorsão mediante sequestro, devendo a requisição ser atendida pelos órgãos do poder público ou empresa da iniciativa privada em até 24 (vinte e quatro) horas (Brasil, 1941).

Já o artigo 13-B contém previsão específica à prevenção e à repressão de crimes relacionados ao tráfico de pessoas, ao estipular que, mediante autorização judicial, as empresas prestadoras de serviço de telecomunicações e/ou telemática devem disponibilizar "imediatamente os meios técnicos adequados – como sinais, informações e outros – que permitam a localização da vítima ou dos suspeitos do delito em curso" (Brasil, 1941, art. 13-B, título II, livro I).

Assim, o artigo 13-B permite o rastreamento de sinais de telecomunicação de forma instantânea para fins de prevenção e repressão de atos relacionados ao tráfico de pessoas.

A Lei n. 13.344/2016 produzida em solo nacional se insere, em verdade, dentro de esforço coletivo internacional para enfrentamento do tráfico de pessoas, que é plasmado pelo Protocolo Adicional à Convenção das Nações Unidas contra o Crime Organizado Transnacional Relativo à Prevenção, Repressão e Punição do Tráfico de Pessoas, em Especial Mulheres e Crianças (Ramos, 2024).

Segundo tal Protocolo (promulgado em solo brasileiro pelo Decreto n. 5.018/04), os Estados signatários devem tomar medidas para prevenir o tráfico de pessoas, em especial de mulheres e crianças, além de proteger e ajudar as vítimas e cooperar entre si para tais finalidades. Inclusive, o Protocolo prevê a obrigação, em seu artigo 5º, de criminalização do tráfico de pessoas, a refletir obrigações processuais penais positivas aos Estados, revelando a característica de a segurança pública não ser apenas um direito fundamental e humano negativo, mas também de índole positiva, com deveres de ação pelo Estado e direito dos ofendidos em exigir a tutela estatal (Ramos, 2024).

Referido Protocolo contava, em 2023, com 181 Estados partes (Ramos, 2024).

Não é por acaso, então, que as previsões legislativas entre Portugal e Brasil quanto ao tráfico de pessoas sejam similares, nem o é a inclusão da localização de vítimas de tráfico de pessoas como causa a justificar a utilização da identificação biométrica à distância em tempo real, uma vez que se trata de imperativo internacional prevenir e reprimir tais tipos de conduta, que, além de extremamente reprováveis, assumem características transnacionais, a exigir esforços conjuntos dos países.

Logo, a identificação biométrica à distância em tempo real, nessa situação, insere-se dentro desse contexto de enfrentamento do tráfico de pessoas, em que há normativas internacionais exigindo a ação dos Estados contra tais condutas. A tecnologia, nesse ponto, então, aprofunda os esforços estatais no intuito de cumprir a obrigação processual penal positiva existente.

O último delito mencionado para fins de localização de vítima se trata de "exploração sexual".

Em busca ao Código Penal Português, não se localizou um tipo penal independente de "exploração sexual". Embora exista o capítulo V denominado "Dos crimes contra a liberdade e autodeterminação sexual", com artigos de 163 a 179, não há tipificação específica de "exploração sexual" (Portugal, 1995).

Em verdade, em consulta ao termo "exploração sexual", os únicos resultados obtidos foram no tipo penal de "Tráfico de pessoas", constante no artigo 160 do referido Código, acima mencionado (Portugal, 1995).

Logo, considera-se que a previsão "exploração sexual" revolve o contexto de tráfico de pessoas ou o próprio crime de rapto, que, tipificado no artigo 161 do Código Penal Português, também pode ser direcionado contra liberdade e autodeterminação sexual da vítima.

Percebe-se, dessa forma, que a tecnologia vai se direcionar à localização de vítimas de tráfico de pessoas ou cuja liberdade foi restringida contra sua vontade por rapto.

Embora possa se discutir se referidas tipificações são ou não *numerus clausus*, é certo que o próprio Regulamento permitiu abertura semântica ao prever que a tecnologia também poderia ser utilizada para localização de pessoas desaparecidas.

Considera-se que referida previsão, ao não especificar a situação de desaparecimento, permite maior maleabilidade na hipótese de aplicação da identificação biométrica à distância em tempo real, bastando a demonstração de que a pessoa visada está desaparecida.

O desaparecimento, por sua vez, pode decorrer de diversas situações distintas, podendo ou não envolver fato criminoso prévio.

Essa abertura semântica é importante para garantir que determinadas situações não sejam excluídas da possibilidade de aplicação da tecnologia por falta de permissão normativa expressa, evitando questionamentos judiciais. Relembra-se, aqui, que as circunstâncias fáticas

não raras vezes apresentam complexidades próprias, cuja antecipação pelo legislador se torna improvável.

Além disso, é fundamental se ter em mente que a vinculação a determinados crimes acarretaria a necessidade de demonstração da ocorrência de tais delitos, o que, por vezes, pode ser de difícil comprovação *ex ante*, sem localização da vítima, a reforçar a importância da previsão genérica de localização de pessoas desaparecidas, que funciona como verdadeiro *soldado de reserva*.

Sobre essa primeira hipótese de aplicação da tecnologia, rememora-se o exposto anteriormente, em que a ONG americana Thorn, que, mediante emprego de reconhecimento facial, teria conseguido resgatar mais de 10 mil crianças vítimas de tráfico sexual (Oliveira *et al.*, 2022), ou o fato de que a polícia da Índia indiciou que, em 2018, o uso de tecnologia de reconhecimento facial permitiu a identificação de 3000 crianças desaparecidas em somente 4 dias (Zalnieriute, 2024).

Verifica-se, portanto, que essa primeira hipótese prevê a aplicação da tecnologia em benefício à pessoa visada, o que, certamente, mitiga diversas das críticas doutrinárias analisadas anteriormente, pautadas primordialmente no ponto de que a tecnologia prejudicaria os abordados.

Ademais, como exposto, essa hipótese de uso se encontra dentro de esforço para prevenção e repressão do tráfico de pessoas, que demanda ações positivas pelos Estados para proteção das vítimas.

A segunda hipótese de aplicação envolve a "prevenção de uma ameaça específica, substancial e iminente à vida ou à segurança física de pessoas singulares ou de uma ameaça real e atual ou real e previsível de um ataque terrorista" (União Europeia, 2024, p. 52).

Trata-se, então, de medida direcionada à prevenção de crimes.

Por isso, a ameaça da ocorrência de delito deve ser "específica, substancial e iminente à vida ou à segurança física de pessoas singulares ou ser real e atual ou real e previsível de um ataque terrorista" (União Europeia, 2024, p. 52).

Quando a ameaça for direcionada a pessoas singulares, não é definido especificamente o crime a ser cometido, apenas que ele seja direcionado contra a vida ou a segurança física, o que deixa margem para inclusão de diversos delitos, cuidando-se de redação aberta.

Por outro lado, tratando-se de ameaça a coletividade indeterminada, o dispositivo prevê que seja um ataque terrorista.

Sobre mencionada circunstância, o ordenamento português tipifica o crime de terrorismo na Lei n. 52/2003, criminalizando, conforme artigo 3º, quem promover ou funda grupo terrorista ou adere a ele. O conceito de grupo terrorista se encontra no artigo 2º da referida Lei (Portugal, 2003).

Aqui a hipótese de incidência é mais restrita, porquanto direcionada a ataques terroristas, cuja tipificação se encontra na Lei Portuguesa n. 52/2003 (o Brasil também possui lei específica para tipificação do terrorismo, a saber, a Lei n. 13.260/16).

Nessa segunda hipótese de aplicação, então, busca-se a prevenção de ameaças, evitando-se que elas ocorram. Justifica-se a incidência da tecnologia exatamente para evitar que vidas ou a segurança física das pessoas sejam lesadas pela concretização da ameaça séria e real existente.

A terceira hipótese de aplicação da tecnologia diz respeito a (União Europeia, 2024, p. 52):

> iii) localização ou identificação de uma pessoa suspeita de ter cometido uma infração penal, para efeitos da realização de uma investigação criminal, ou instauração de ação penal ou execução de uma sanção penal por alguma das infrações referidas no anexo II e puníveis no Estado-Membro em causa com pena ou medida de segurança privativa de liberdade de duração máxima não inferior a quatro anos.

Como se vê, a pessoa visada é, nessa hipótese, ou suspeita de infração penal ou condenada por infração penal, de modo que a intenção não é a prevenção, mas a repressão do delito, já ocorrido.

As infrações penais estão listadas no anexo II, cuja pena máxima não pode ser inferior a quatro anos. O anexo II conta com a seguinte lista de infrações (União Europeia, 2024, p. 126):

> Infrações penais a que se refere o artigo 5.o, n.o 1, primeiro parágrafo, alínea h), subalínea iii):
>
> — Terrorismo;
>
> — Tráfico de seres humanos;

> — Exploração sexual de crianças e pornografia infantil;
>
> — Tráfico de estupefacientes e substâncias psicotrópicas;
>
> — Tráfico de armas, munições ou explosivos;
>
> — Homicídio, ofensas corporais graves;
>
> — Tráfico de órgãos ou tecidos humanos;
>
> — Tráfico de materiais nucleares ou radioativos;
>
> — Rapto, sequestro ou tomada de reféns;
>
> — Crimes abrangidos pela jurisdição do Tribunal Penal Internacional;
>
> — Desvio de aviões ou navios;
>
> — Violação;
>
> — Criminalidade ambiental;
>
> — Roubo organizado ou à mão armada;
>
> — Sabotagem;
>
> — Participação numa organização criminosa envolvida numa ou mais das infrações acima enumeradas.

Como se percebe, o Regulamento limitou a incidência para localização de suspeitos ou condenados a casos de infrações pré-determinadas (*numerus clausus*), com gravidade considerável (pena máxima não inferior a 4 anos).

Portanto, não é para qualquer suspeito ou condenado que será possível a utilização da tecnologia, mas somente nos casos listados nessa terceira hipótese.

Um ponto importante sobre as hipóteses de incidência da tecnologia, referente ao fato de o Regulamento estar inserido no Novo Quadro Legislativo, é que a Comissão Europeia pode atualizar a lista de práticas proibidas, conforme artigo 112 do Regulamento, evitando eventual defasagem em razão do transcurso do tempo, de evoluções tecnológicas ou de mudanças sociais (União Europeia, 2024).

Logo, apesar dessas hipóteses de incidência inicialmente previstas, há possibilidade de avaliação e reexame pela Comissão Europeia, o que demonstra o contínuo monitoramento de aplicação da tecnologia, em acordo com o exposto anteriormente sobre o ciclo de vida da inteligência artificial.

Mais alguns pontos são pertinentes para análise das hipóteses de incidência da tecnologia.

Segundo item 2 da alínea *h*, o uso deve ser feito apenas para confirmar a identidade de determinada pessoa especificamente visada (União Europeia, 2024).

Assim, não é possível utilizar a tecnologia sem já se ter delimitado qual a pessoa se pretende identificar.

Isso é extremamente relevante, pois veda possibilidades de uso da tecnologia que são criticadas pela doutrina.

Em decorrência, não será possível a identificação biométrica à distância em tempo real para finalidades preditivas (Dushi, 2020), na medida em que essa não dispõe *ex ante* do alvo (afinal no policiamento preditivo trabalha-se com prognósticos), nem será permitida a identificação biométrica de número sem precedentes de pessoa, fortemente criticada por Hirose (2017).

Aliás, a necessidade de que o reconhecimento facial seja direcionado à pessoa específica, vedando-se o uso para identificação de faces não determinadas, é reforçada pela vedação da alínea *e* do artigo 5º, que proíbe "sistemas de IA que criam ou expandem bases de dados de reconhecimento facial através da recolha aleatória de imagens faciais a partir da Internet ou de imagens de televisão em circuito fechado (TVCF)" (União Europeia, 2024, p. 51).

Em semelhante toada, é pertinente observar o item 42 do preâmbulo, que prestigia o princípio da presunção de inocência e assinala que as pessoas serão avaliadas em razão de seu comportamento real. Conforme tal enunciado, "pessoas singulares nunca poderão ser julgadas com base no comportamento previsto pela IA com base exclusivamente na definição do seu perfil, nos traços ou características da sua personalidade" (União Europeia, 2024, p. 12).

Assim, o uso da tecnologia deve ter alvo específico, fundado em circunstâncias decorrentes de seu comportamento real e não baseado em julgamentos preditivos ou com base em meras características pessoais.

Essa questão é trabalhada por Mobilio (2023), ao assinalar que a tecnologia, em tese, pode ser voltada para identificação de pessoas, grupos ou para escanear toda a sociedade. É certo que, quanto maior for a abrangência do alvo, maiores serão os riscos inerentes ao uso da tecnologia (Mobilio, 2023).

Verifica-se que apenas a identificação de pessoas individualizadas e pré-determinadas é permitida pelo Regulamento; logo, a tecnologia não pode ter como alvo grupos ou a inteira sociedade.

Ademais, é fundamental ressaltar o item 38 do preâmbulo, no sentido de que as hipóteses excepcionais previstas no Regulamento direcionadas à identificação biométrica à distância em tempo real se configuram lei especial para tratamento de dados em relação às regras gerais previstas no artigo 10 da Diretiva (UE) 2016/680 (União Europeia, 2024). Assim, o tratamento de dados seguirá as disposições do Regulamento da Inteligência Artificial, quando direcionado à identificação biométrica à distância em tempo real.

Acontece que o mero preenchimento de alguma das hipóteses de uso da tecnologia e a prévia identificação da pessoa visada não é suficiente para validar a utilização da tecnologia.

Como assinalado, o uso deve ser estritamente necessário.

Isso implica na observância de balizas fixadas previamente pelo Regulamento, que definem quando esse uso é realmente estritamente necessário, o que será analisado a seguir.

4.5. BALIZAS E PROCEDIMENTO PARA DEFERIMENTO

A necessidade de uso estritamente necessário da identificação biométrica à distância em tempo real é adiantada pelo item 34 do preâmbulo, que assim dispõe (União Europeia, 2024, p. 10):

> A fim de assegurar que esses sistemas sejam utilizados de uma forma responsável e proporcionada, também importa estabelecer que, em cada uma dessas situações enunciadas exaustivamente e definidas de modo restrito, é necessário ter em conta determinados elementos, em especial no que se refere à natureza da situação que dá origem ao pedido e às consequências da utilização para os direitos e as liberdades de todas as pessoas em causa e ainda às salvaguardas e condições previstas para a utilização. Além disso, a utilização de sistemas de identificação biométrica à distância «em tempo real» em espaços acessíveis ao público para efeitos de aplicação da lei só deverá ocorrer para efeitos de confirmação da identidade de uma pessoa especificamente visada e deverá ser limitada ao estritamente necessário no que respeita ao período, bem como ao âmbito geográfico e pessoal, tendo em conta, especialmente, os dados ou indícios relativos às ameaças, às vítimas ou ao infrator. A utilização do sistema de identificação biométrica à distância em tempo real em espaços acessíveis ao público só deverá ser autorizada se a competente autoridade responsável pela aplicação da lei tiver concluído uma

> avaliação de impacto sobre os direitos fundamentais e, salvo disposição em contrário no presente regulamento, tiver registado o sistema na base de dados prevista no presente regulamento. A base de dados de pessoas utilizada como referência deverá ser adequada a cada utilização em cada uma das situações acima indicadas.

Além de alguma das finalidades previstas na alínea *h* (busca de vítimas e pessoas desaparecidas, prevenção de ameaça específica contra pessoa ou real de ataque terrorista, e localização de suspeito ou condenado por infração grave) e definição do alvo, o item 2 da referida alínea dispõe sobre os elementos que devem ser preenchidos para demonstrar que o uso da tecnologia, dado o seu grau de intrusão em direitos, é estritamente necessário (União Europeia, 2024).

Nessa senda, o item 2 aponta que, para uso da tecnologia, devem ser considerados os seguintes elementos (União Europeia, 2024, p. 52):

> a) A natureza da situação que origina a possível utilização, em especial a gravidade, a probabilidade e a magnitude dos danos causados na ausência da utilização do sistema;
>
> b) As consequências da utilização do sistema para os direitos e as liberdades de todas as pessoas afetadas, em especial a gravidade, a probabilidade e a magnitude dessas consequências.

O dispositivo revela verdadeira ponderação para autorizar o uso da tecnologia.

Isso porque devem ser considerados os prejuízos, caso não seja utilizado o sistema, e ponderado com as consequências da utilização do sistema para as pessoas afetadas. Em resumo, busca-se verificar se os benefícios da utilização da identificação biométrica à distância em tempo real para o caso específico superam seus potenciais prejuízos, o que se trata, a rigor, da proporcionalidade em sentido estrito.

Nos termos da lição de Alexy (1997), a proporcionalidade em sentido estrito pauta-se na ponderação entre o fim atingido e o princípio violado, de modo a justificar a interferência em determinado direito pelo maior grau de satisfação de outro fim igualmente valioso em termos jurídicos.

Revela-se, então, evidente que o Regulamento Europeu, ao estabelecer a necessidade de ponderação entre as consequências do uso da tecnologia e os danos que poderiam ocorrer caso

não houvesse o uso, prestigia a realização de teste de proporcionalidade em termos semelhantes ao preconizado por Alexy (1997).

Logo, para cada caso, deve haver essa ponderação individualizada.

Além disso, o sistema de identificação biométrica à distância em tempo real deve, nos termos do último parágrafo do item 2 da alínea *h* do artigo 5º, ser submetido à prévia avaliação de impacto sobre os direitos fundamentais para ser utilizado, com registro na base de dados da União Europeia (União Europeia, 2024).

A avaliação de impacto sobre direitos fundamentais já foi mencionada e está prevista no artigo 27 do Regulamento (União Europeia, 2024).

Os sistemas listados no anexo III, dos quais constam a identificação biométrica à distância e aqueles utilizados para segurança pública, devem realizar avaliação de impacto em direitos fundamentais como previsto no artigo 27 (União Europeia, 2024), o que reflete, em essência, um verdadeiro teste de ponderação para verificar se o uso da inteligência artificial se mostra adequado, necessário e proporcional em sentido estrito para as finalidades visadas à vista dos direitos impactados.

Essa avaliação, nos termos do artigo 27, deve incluir descrição dos processos pelos quais o sistema seja utilizado conforme a finalidade pretendida, descrição do período e frequência de utilização previstos, categorias de pessoas singulares ou grupos suscetíveis de serem afetados com os riscos de danos em face de tais pessoas ou grupos, descrição das medidas de supervisão humana do sistema e medidas a serem tomadas caso os riscos previstos se materializem (União Europeia, 2024).

Isso significa, para os casos de identificação biométrica à distância em tempo real, que a avaliação deve considerar os aspectos tecnológicos e jurídicos apontados anteriormente na presente obra.

Logo, devem ser considerados, sob o ponto de vista técnico, a inexistência de neutralidade da tecnologia, o *trade-off threshold* (falsos positivos/falsos negativos), qualidade de dados (banco de dados), vieses (erro algorítmico e localização das câmeras), a necessidade de supervisão humana, e, sob o ponto de vista jurídico, devem ser levadas em conta as seguintes interferências: autonomia/privacidade (qualidade de dados e consenso), direitos à liberdade de expressão e à reunião (*chilling effect*), discriminação, princípio da presunção de inocência, princípios da transparência e da explicabilidade, grupos etários (crianças e idosos).

Essa avaliação de impacto, nos termos do item 2 do artigo 27, será atualizada caso houver alguma mudança nas informações inicialmente avaliadas (União Europeia, 2024). Isso permite o constante monitoramento e revisão do sistema.

Como se percebe, a avaliação de impacto sobre direitos fundamentais, diferentemente da ponderação anteriormente assinalada (que é feita caso a caso), é realizada sobre o sistema inteiro, de forma prévia ao uso, englobando os usos pretendidos.

Nessa senda, enquanto para cada caso individualizado haverá ponderação particular dos benefícios e prejuízos, o sistema como um todo deve passar previamente por avaliação de impacto sobre direitos fundamentais, considerando os usos pretendidos, isto é, as três hipóteses excepcionais de uso mencionadas no subcapítulo anterior.

É claro, contudo, que pode se optar pela limitação do uso a alguma das hipóteses, não englobando todas; apenas não é possível expandir as possibilidades de uso para além das hipóteses mencionadas no subcapítulo anterior (localização de vítimas ou pessoas desaparecidas, prevenção de ameaça real e séria, localização de suspeito ou condenado por crime grave).

Nessa senda, aliás, o item 5 da alínea *h* do artigo 5º estipula que os Estados-Membros da União Europeia podem autorizar total ou parcialmente as hipóteses excepcionais de uso da identificação biométrica à distância em tempo real, inclusive indicando quais delitos do anexo III justificam o uso da tecnologia (União Europeia, 2024).

Logo, apesar da previsão do Regulamento, os Estados, por meio de sua legislação interna, podem limitar as hipóteses de incidência da tecnologia; não podem, por outro lado, ampliar as hipóteses.

Aos Estados cabe, ainda, criar as regras para autorização judicial (o que será abordado a seguir), comunicando à Comissão no prazo de 30 dias as regras referentes à utilização do sistema de identificação biométrica à distância (União Europeia, 2024).

Sobre o tema, inclusive, é pertinente reproduzir o teor do item 37 do preâmbulo do Regulamento (União Europeia, 2024, p. 11):

> Além disso, no âmbito do regime exaustivo estabelecido pelo presente regulamento, importa salientar que essa utilização no território de um Estado-Membro em conformidade com o presente regulamento apenas deverá ser possível uma vez que o Estado-Membro em causa tenha decidido possibilitar expressamente a autorização dessa utilização nas regras de execução previstas

> no direito nacional. Consequentemente, ao abrigo do presente regulamento, os Estados-Membros continuam a ser livres de não possibilitar essa utilização ou de apenas possibilitar essa utilização relativamente a alguns dos objetivos passíveis de justificar uma utilização autorizada identificados no presente regulamento. Essas regras nacionais deverão ser comunicadas à Comissão no prazo de 30 dias a contar da sua adoção.

Além da avaliação, o sistema de identificação biométrica à distância em tempo real deve ser registrado na base de dados da União Europeia, nos termos previstos pelo artigo 49 do Regulamento (União Europeia, 2024).

Segundo tal dispositivo, os sistemas de risco elevado enumerados no anexo III, no qual se inclui a identificação biométrica à distância e a atividade de segurança pública, antes de serem colocados no mercado, devem ser registrados na base de dados da União Europeia (União Europeia, 2024).

Inclusive, para a atividade de segurança pública, o registro será realizado em seção segura e não pública, com acesso apenas à Comissão Europeia e as autoridades nacionais, nos termos do item 4 do artigo 49, exatamente pelos dados operacionais sensíveis existentes, definidos assim pelo artigo 3º, item, 38, do Regulamento: "dados operacionais relacionados com atividades de prevenção, deteção, investigação ou repressão de infrações penais, cuja divulgação possa comprometer a integridade de processos penais" (União Europeia, 2024, p. 25).

Logo, o registro do sistema na base de dados europeu apresenta limitações de publicidade exatamente pelas finalidades de segurança pública, envolvendo muitas vezes dados sigilosos.

A previsão normativa da base de dados se encontra no artigo 71 do Regulamento (União Europeia, 2024).

Embora o sistema, com sua avaliação de impacto, deva ser registrado, em regra, previamente ao uso, o artigo 5º, alínea *h*, permite que, "em casos de urgência devidamente justificados, a utilização desses sistemas pode ser iniciada sem o registo na base de dados da UE, desde que esse registo seja concluído sem demora injustificada" (União Europeia, 2024, p. 52).

Assim, em situações excepcionais, devidamente justificadas pela urgência, é possível a utilização do sistema sem o registro prévio na base de dados, contanto esse registro seja concluído posteriormente sem demora.

É interessante pontuar, ainda, que a utilização do sistema não pode infringir outra legislação da União Europeia, conforme artigo 5º, alínea *h*, n. 8, do Regulamento (União Europeia, 2024).

Não bastasse o cumprimento das balizas, cada uso deverá ser autorizado de maneira individualizada.

Nos termos do item 3 da alínea *h*, cada utilização do sistema "está sujeita a autorização prévia concedida por uma autoridade judiciária, ou uma autoridade administrativa independente cuja decisão seja vinculativa, do Estado-Membro" (União Europeia, 2024, p. 52).

Logo, não basta o cumprimento das balizas acima mencionadas, como também deve haver autorização judicial prévia[15].

Como adiantado, a legislação nacional deve prever o procedimento para realização desse pedido de autorização individualizado para o uso da tecnologia.

O pedido conterá fundamentação acerca da pertinência do uso da tecnologia, demonstrando o cumprimento das balizas previamente expostas.

A autorização será concedida apenas com dados objetivos ou indícios claros justificantes da utilização do sistema (União Europeia, 2024). O pedido de autorização deve, então, vir lastreado por elementos probatórios mínimos justificadores da utilização do sistema.

O pedido também dever se limitado "ao estritamente necessário no que diz respeito ao período de tempo e ao âmbito geográfico e pessoal" (União Europeia, 2024, p. 52).

Isso exatamente porque o sistema é utilizado de forma restritiva, com individualização do alvo, não podendo abranger pessoas indeterminadas. Cuida-se, portanto, de corolário lógico que o requerimento de autorização para uso apresente limitações em termos temporais, geográficos e pessoais, de modo a não resvalar para autorização genérica.

Essa previsão revela que o uso realmente ocorrerá da forma estritamente necessária para a finalidade pretendida pela hipótese de incidência, visando a atingir o objetivo proposto.

---

15 Menciona-se autorização judicial apenas, pois, no Brasil, inexiste, a rigor, autoridade administrativa independente cuja decisão seja vinculativa, nos termos do art. 5º, XXXV, da Constituição Federal (Brasil, 1988).

É interessante salientar, ainda, que não podem ser tomadas decisões com efeitos jurídicos adversos somente “com base nos resultados saídos do sistema de identificação biométrica à distância ‘em tempo real’” (União Europeia, 2024, p. 53).

Isso representa, além da necessidade de supervisão humana, o respeito ao princípio da presunção de inocência e a observância do devido processo legal, em que a conclusão sobre a culpa de uma pessoa depende de procedimento formalizado com direito a contraditório e a ampla defesa.

Além disso, conforme item 4, cada uso deve ser comunicado à autoridade de fiscalização do mercado pertinente e à autoridade nacional de proteção de dados, contendo informações acerca da utilização (União Europeia, 2024).

Conforme item 6 da alínea *h*, as autoridades nacionais devem apresentar relatórios anuais à Comissão Europeia sobre o uso da tecnologia, com o número de decisões tomadas pelas autoridades judiciais competentes sobre a utilização (União Europeia, 2024).

Assim, a comunicação prevista no item 4 deve conter, pelo menos, as informações mínimas a serem repassadas posteriormente à Comissão Europeia (União Europeia, 2024).

Com base nesses dados, a Comissão Europeia publica relatórios anuais sobre o uso da tecnologia; tais relatórios não podem conter dados operacionais sensíveis sobre as atividades de segurança pública, isto é: “dados operacionais relacionados com atividades de prevenção, deteção, investigação ou repressão de infrações penais, cuja divulgação possa comprometer a integridade de processos penais”, nos termos artigo 3º, item, 38, do Regulamento (União Europeia, 2024, p. 48).

Percebe-se, portanto, que o cumprimento das balizas antes assinaladas e a verificação da pertinência do uso da tecnologia para as hipóteses excepcionais, com base em elementos probatórios mínimos acerca da presença de causa justificadora, passa por autorização judicial prévia, de modo a permitir o uso ao estritamente necessário em termos temporais, geográficos e pessoais.

Embora a regra seja de autorização judicial prévia, é possível que referida autorização ocorra posteriormente em situação de urgência devidamente justificada, devendo, contudo, ser solicitada no prazo máximo de 24 horas (União Europeia, 2024). De qualquer sorte, se, em tais circunstâncias, a autorização for negada, a utilização deve ser imediatamente suspensa e os resultados prontamente descartados e eliminados (União Europeia, 2024).

Logo, além das balizas especiais para identificação biométrica à distância em tempo real, a utilização em si do sistema depende de autorização judicial prévia e individualizada para cada caso, oportunidade em que se avalia tanto a pertinência do sistema para a situação específica quanto à ponderação entre prejuízos e benefícios no caso concreto.

Certamente, então, as situações de incidência da tecnologia serão estritamente limitadas, ante as hipóteses de uso restritas, as balizas especiais de observância e a necessidade de prévia autorização judicial calcada em requerimento fundamentado com elementos probatórios mínimos e limitação temporal, geográfica e pessoal.

Além desses requisitos específicos, incidentes especialmente para identificação biométrica à distância em tempo real aplicada para segurança pública, é fundamental salientar que o uso do sistema ainda será submetido aos demais requisitos dos sistemas de risco elevado (União Europeia, 2024).

Isso porque, como visto, se cuida de sistema inserto na área de segurança pública, atividade constante no item 6 do anexo III, além de envolver identificação biométrica à distância, que consta no item 1, *a*, do anexo III (União Europeia, 2024).

A existência de risco elevado do sistema de identificação biométrica à distância é justificada pelo item 54 do preâmbulo, segundo o qual as "inexatidões técnicas dos sistemas de IA concebidos para a identificação biométrica à distância de pessoas singulares podem conduzir a resultados enviesados e ter efeitos discriminatórios" (União Europeia, 2024, p. 15).

Portanto, o sistema deve observar, dentre outros, os seguintes dispositivos: Implementação de gestão de risco (artigo 9º); Governança de dados (artigo 10); Elaboração de documentação técnica (artigo 11); Manutenção de registros (artigo 12); Transparência e informação pelos desenvolvedores aos implantadores (artigo 13); Supervisão humana (artigo 14); Exatidão, solidez e cibersegurança (artigo 15) (União Europeia, 2024).

Ainda, eles são submetidos à avaliação de conformidade para recebimento da marca "CE" (artigo 48) (União Europeia, 2024).

O item 59 do preâmbulo do Regulamento contém considerações importantes sobre a utilização em geral de inteligência artificial para atividades de segurança pública. Se não, veja-se o teor do mencionado dispositivo (União Europeia, 2024, p. 17):

Tendo em conta o papel e a responsabilidade das autoridades responsáveis pela aplicação da lei, as suas ações que implicam certas utilizações dos sistemas de IA são caracterizadas por um grau substancial de desequilíbrio de poder e podem conduzir à vigilância, detenção ou privação da liberdade de uma pessoa singular, bem como ter outras repercussões negativas nos direitos fundamentais garantidos pela Carta. Em particular, se não for treinado com dados de alta qualidade, não cumprir os requisitos adequados em termos de desempenho, de exatidão ou solidez, ou não tiver sido devidamente concebido e testado antes de ser colocado no mercado ou em serviço, o sistema de IA pode selecionar pessoas de uma forma discriminatória, incorreta ou injusta. Além disso, o exercício de importantes direitos fundamentais processuais, como o direito à ação e a um tribunal imparcial, o direito à defesa e a presunção de inocência, pode ser prejudicado, em particular, se esses sistemas de IA não forem suficientemente transparentes, explicáveis e documentados. Como tal, é apropriado classificar como sendo de risco elevado, na medida em que a sua utilização seja permitida nos termos do direito da União e o direito nacional aplicáveis, vários sistemas de IA que se destinam a ser utilizados no contexto da aplicação da lei, no qual a exatidão, a fiabilidade e a transparência são particularmente importantes para evitar repercussões negativas, manter a confiança do público e assegurar a responsabilidade e vias de recurso eficazes. Tendo em conta a natureza das atividades e os riscos associados às mesmas, esses sistemas de IA de risco elevado deverão incluir, em particular, sistemas de IA concebidos para serem utilizados por autoridades responsáveis pela aplicação da lei ou por instituições, órgãos ou organismos da União, ou em seu nome, em apoio das autoridades responsáveis pela aplicação da lei para avaliar o risco de uma pessoa singular vir a ser vítima de infrações penais, como polígrafos e instrumentos semelhantes, para avaliar a fiabilidade dos elementos de prova no decurso da investigação ou da repressão de infrações penais, e, na medida em que tal não seja proibido nos termos do presente regulamento, para avaliar o risco de uma pessoa singular cometer uma infração ou reincidência não apenas com base na definição de perfis de pessoas singulares ou na avaliação os traços e características da personalidade ou do comportamento criminal passado de pessoas singulares ou grupos, para a definição de perfis no decurso da deteção, investigação ou repressão de infrações penais. Os sistemas de IA especificamente concebidos para serem utilizados em processos administrativos por autoridades fiscais e aduaneiras, bem como por unidades de informação financeira que desempenhem funções administrativas de análise de informações nos termos do direito da União em matéria de combate ao branqueamento de capitais, não deverão ser classificados como sistemas de IA de risco elevado utilizados por autoridades responsáveis pela aplicação da lei para efeitos de prevenção, deteção, investigação e repressão de infrações penais. A utilização de ferramentas de IA pelas autoridades responsáveis pela aplicação da lei e por outras autoridades pertinentes não deverá tornar-se um fator de desigualdade nem de exclusão. Não se deverá descurar o impacto da utilização de ferramentas de IA nos direitos de defesa dos suspeitos, nomeadamente a dificuldade de obter informações significativas sobre o funcionamento desses sistemas e a dificuldade daí resultante de contestar os seus resultados em tribunal, em particular quando se trate de pessoas singulares sob investigação.

Em primeiro plano, pontua-se a situação de assimetria de poder e a potencialidade de repercussões negativas a direitos fundamentais, notadamente pelas consequências de vigilância, detenção e privação de liberdade que a tecnologia pode levar.

Em seguida, destaca-se a importância de treinamento do sistema com dados de alta qualidade, bem como a observância de critérios de desempenho, exatidão e solidez, sobretudo para evitar vieses discriminatórios, o que foi abordado de forma extensiva anteriormente no presente trabalho.

Aponta-se, ademais, a necessidade de observância dos princípios incidentes na seara penal, em especial da presunção de inocência, da ampla defesa e de julgamento por julgador imparcial, ressaltando-se a importância de transparência e explicabilidade do sistema.

Por conta desses fatores, o referido dispositivo conclui pela necessidade de classificação geral do emprego de inteligência artificial na atividade de segurança pública como de risco elevado.

Logo, se o sistema de inteligência artificial usado na segurança pública não for de risco proibido (isto é, não esteja listado em alguma das hipóteses do artigo 5º do Regulamento), ele será, em regra, de risco elevado, exatamente como ocorre com a identificação biométrica à distância nas hipóteses permitidas, impondo, consequentemente, o cumprimento dos diversos deveres correlatos para os implantadores de sistemas de risco elevado (União Europeia, 2024).

O item 73 do preâmbulo, por sua vez, aborda a necessidade de supervisão humana dos sistemas de risco elevado (União Europeia, 2024), outro ponto já tratado nesse trabalho. Referido item enfatiza a importância da existência de restrições operacionais para que o sistema não anule a interferência humana, bem como destaca que o operador deve ter competências específicas para desempenhar essa atividade (União Europeia, 2024).

Mais relevante é que o item 73 traz a seguinte previsão em caso de falsa correspondência pelo sistema de identificação biométrica (União Europeia, 2024, p. 21):

> [...] Tendo em conta as consequências significativas para as pessoas em caso de uma correspondência incorreta por determinados sistemas de identificação biométrica, é conveniente prever um requisito reforçado de supervisão humana para esses sistemas, de modo a que o responsável pela implantação não possa tomar qualquer medida ou decisão com base na identificação resultante do sistema, a menos que tal tenha sido verificado e confirmado separadamente por, pelo menos, duas pessoas singulares. [...].

Portanto, a supervisão humana deve ser reforçada na identificação biométrica à distância em tempo real, inclusive mediante confirmação por, pelo menos, duas pessoas singulares separadamente, conforme prevê o artigo 14, item 5, do Regulamento, em linha ao exposto no preâmbulo (União Europeia, 2024). Contudo, o próprio artigo 14, item 5, prevê que esse requisito pode deixar de ser aplicado para fins de segurança pública caso o direito da União Europeia ou o direito nacional o considere desproporcional (União Europeia, 2024).

Com base no apurado, verifica-se que a utilização da identificação biométrica à distância em tempo real se sujeita a balizas estreitas, a procedimento rigoroso, limitado a hipóteses específicas e preenchimento de requisitos criteriosos.

Feita essa análise, cumpre averiguar se a normatização europeia se mostra de acordo com os direitos humanos em jogo.

4.6. COMPATIBILIDADE DO REGULAMENTO COM OS DIREITOS HUMANOS

Nos subcapítulos anteriores, o estudo restringiu-se a descrever as previsões normativas do Regulamento Europeu acerca do uso da identificação biométrica à distância em tempo real para fins de segurança pública.

Como foi possível constatar, o Regulamento contém detalhado arcabouço normativo sobre o uso de inteligência artificial para tal finalidade.

No presente subcapítulo, por sua vez, analisa-se se a normatização europeia se mostra de acordo com os direitos humanos em voga.

Não serão aqui analisadas as críticas no sentido de banimento peremptório da tecnologia, porquanto estas já foram abordadas anteriormente no presente trabalho. A partir daqui, assume-se a posição de que a identificação biométrica à distância em tempo real é passível, em tese, de regulação, de modo que o foco se referirá às críticas específicas à forma pela qual tal regulação foi realizada pelo Regulamento.

A Agência da União Europeia para Direitos Fundamentais, ao concluir estudo sobre o tema, apontou que o uso da referida tecnologia, mais desafiadora ocorrer em espaços públicos e em tempo real, deveria ser estritamente limitada ao combate de terrorismo e outras formas de

crimes graves, bem como para encontrar pessoas ou vítimas de crimes, e dependeria de regulamentação clara e suficientemente detalhada, indicando quando o processamento de imagens faciais se revelaria necessário e proporcional, além de preconizar salvaguardas para proteger os indivíduos de consequências negativas do sistema (FRA, 2020).

Nessa linha, a Agência da União Europeia para Direitos Fundamentais aponta que as tecnologias, embora utilizadas em finalidades públicas, são desenvolvidas por empresas particulares, que devem incluir, no processo de confecção do sistema, preocupações com proteção de dados e direitos fundamentais, contratando peritos nas áreas, de modo a garantir a adequação do desenho da inteligência artificial aos direitos fundamentais em jogo (FRA, 2020).

Não por outro motivo, então, referida Agência enfatiza que a avaliação de impacto em direitos fundamentais é ferramenta essencial para garantir a observância dos direitos fundamentais envolvidos, cuja realização não pode ser prejudicada por alegações de segredo industrial ou confidencialidade (FRA, 2020). Inclusive, devido à constante evolução tecnológica no tema, torna-se fundamental monitoramento próximo por entidades fiscalizatórias independentes, com suficientes poderes, recursos e conhecimentos (FRA, 2020).

Verifica-se que o Regulamento Europeu da Inteligência Artificial buscou dar eco aos apontamentos da Agência da União Europeia para Direitos Fundamentais, na medida em que estabeleceu disciplina normativa específica e restrita para identificação biométrica à distância em tempo real, direcionada a casos excepcionais e dependente de avaliação de impacto em direitos fundamentais, autorização judicial prévia e ponderação individualizada para cada caso, com limitações geográficas, temporais e pessoais, com comunicações às autoridades nacionais e supervisão da Comissão Europeia.

Apesar desse esforço, a previsão normativa do Regulamento não ficou imune a críticas.

Ao analisar o tema, Dushi (2020) salientou a necessidade de que a regulação da matéria fosse precedida por pesquisas robustas a demonstrar o impacto positivo da tecnologia na segurança pública.

Ocorre que ainda se pende de estudos empíricos sobre a real efetividade dos sistemas de identificação biométrica à distância em tempo real, que, ao operarem em situações não controláveis, apresentam margem de precisão bem inferiores aos sistemas de mera verificação de identidade, de modo que o uso não deveria ser liberado antes de tais estudos (Kuhlmann, 2024).

Uma primeira crítica reside, portanto, na falta de estudos probatórios de que a tecnologia realmente agregue na segurança pública (Kuhlmann, 2024), o que, segundo Dushi (2020), seria fator a justificar a manutenção de banimento do uso.

Sobre a questão do banimento da tecnologia, Lynch (2024) sinaliza que, em meados de 2023, durante a tramitação legislativa, encaminhava-se para a vedação completa de uso da tecnologia, o que era endossado por diversos grupos defensores de direitos humanos na União Europeia, mas o texto final recuou da posição mais restritiva ao permitir o uso na segurança pública em situações restritas.

Embora Lynch (2024) concorde com a regulamentação da tecnologia para situações específicas, a autora salienta aparente vagueza sobre a forma como serão implementadas as hipóteses excepcionais de uso, o que traz preocupações de abusos, até porque, pela redação do Regulamento, passa-se a ideia de que o uso da tecnologia estaria totalmente aprovado para as situações excepcionais, quando estas, na verdade, dependeriam ainda de estudo e esforço legislativo pelos próprios Estados-Membros na redação de suas legislações internas.

A autora, assim, salienta que o Regulamento não encerrou todas as discussões sobre o uso da tecnologia, enfatizando a existência ainda de margem de apreciação aos Estados, o que pode, eventualmente, resultar em abusos (Lynch, 2024).

Nada obstante, Lynch (2024, p. 12, tradução nossa) considera o Regulamento a melhor representação de regulação robusta da matéria:

> Embora o Regulamento Europeu da Inteligência Artificial represente a melhor oportunidade para parâmetros robustos, o engajamento com conceitos como limitação proporcional do interesse individual e coletivo na segurança pública e na prevenção criminal foram limitados. Há uma sensação de que, embora haja uma ambição significativa de proteger os direitos individuais e coletivos, como a privacidade e liberdade de expressão, as exclusões para a aplicação da lei são tais que os Estados-Membros têm poder discricionário significativo para usar as formas mais intrusivas de tecnologias de reconhecimento facial.

Além da falta de estudos e da existência de margem nacional para efetiva implementação da tecnologia, um terceiro ponto de crítica consiste no fato de que o Regulamento não se aplica para atividades de defesa, militares e de segurança nacional.

Segundo Lynch (2024), isso aumenta a discricionariedade dos Estados no uso da tecnologia, até porque os conceitos de segurança pública e segurança nacional muitas vezes se confundem em diversos contextos, a tornar a distinção, em termos práticos, complicada.

Aliás, a exclusão da disciplina do Regulamento para a segurança nacional causa preocupações gerais em matéria de direitos humanos (Wiek, 2023).

Conforme Wiek (2023), o Regulamento, embora coerente com as práticas e padrões da Agência da União Europeia para a Cooperação Judiciária Penal (*Eurojust*), revela riscos aos direitos humanos por excluir questões de segurança nacional.

Inclusive, nesse ponto, é pertinente notar a possibilidade de uso duplo da inteligência artificial, no sentido de que a mesma tecnologia pode ser empregada para fins tanto militares quanto civis, o que torna incerta a aplicação do Regulamento (Ruschemeier, 2023).

A solução passaria pela fixação de parâmetros objetivos acerca do que se conceitua como segurança nacional de modo a distingui-la de segurança pública (Wiek, 2023), no intuito de eliminar, ou, pelo menos, minimizar a zona cinzenta salientada por Lynch (2024).

Para fins de identificação biométrica à distância em tempo real, ainda remanesce margem de apreciação nacional para aprovação e implementação do uso, bem como para definição do que é segurança nacional (Wiek, 2023).

Mobilio (2022), apesar de considerar positiva a necessidade de deferimento individualizado de uso, expressa preocupação pela existência de amplitude exacerbada deferida aos Estados para aplicação da tecnologia, o que violaria a necessidade de regras claras e precisas para justificar a interferência em direitos fundamentais.

Em comparação com legislações sobre a matéria realizadas em âmbito federal e estadual dos Estados Unidos, De Hert e Bouchagiar (2024) consideram que o Regulamento Europeu se mostrou dúbio em determinados pontos, o que apresenta potencial de falta de proteção aos direitos fundamentais, bem como de confusão na aplicação da lei.

Segundo os autores, carece-se de menção sobre consenso na regulação europeia, além de haver vagueza quanto a certos deveres e proibições expressamente previstas nas legislações correlatas dos Estados Unidos, notadamente quanto a discriminação, proibição de realização de perfis, balizas de cuidados e de tratamento de dados biométricos sensíveis e confidenciais (De Hert e Bouchagiar, 2024).

Apesar das potenciais alegações de que os pontos de abertura do Regulamento lhe permitem atualização ao longo do tempo, não deixando a normativa engessada, os autores apontam que referidas vaguezas ofereceriam margem para violação a direitos fundamentais e confusão na aplicação da normativa (De Hert e Bouchagiar, 2024).

Prosseguindo nas críticas, Ebers *et al.* (2021) entendem que as hipóteses de exceção que autorizam o uso da tecnologia são demasiadamente largas, pois envolvem não apenas questões temporalmente sensíveis (como encontro de vítimas ou prevenção de ameaças), mas situações sem urgência temporal, como condenados por sentença.

Sobre as hipóteses excepcionais de uso, Smuha *et al.* (2021, p, 26, tradução nossa) também concordam que a regulamentação mostrou excessivamente permissiva, além de não considerar, na visão deles, o *chiiling effect* decorrente da criação de infraestruturas de identificação biométrica à distância:

> Embora reconheçamos que pode haver, em tese, circunstâncias justificadoras da utilização de sistema de identificação biométrica à distância pelas autoridades policiais em espaços públicos em conformidade e com o respeito aos direitos fundamentais, o âmbito das atuais exceções não cumpre o padrão exigido. Em particular, o terceiro fundamento de exceção, que permite a utilização de tal tecnologia para a deteção de autores ou suspeitos de infrações penais, abrange um vasto número de situações. Isso coloca excessivo poder discricionário nas mãos das agências de aplicação da lei. Além disso, as consequências de permitir sistema de identificação biométrica à distância em espaços públicos significam que as infraestruturas que permitirão a utilização permitida desta tecnologia serão construídas e implementadas em grande escala nos Estados-Membros. Uma vez construídas estas infraestruturas, a deformação de função e os aumentos potenciais de usos indevidos ou abusos de tais infraestruturas continuam a ser uma preocupação muito real. É importante sublinhar que os riscos relacionados com esta infraestrutura vão além do impacto na privacidade individual, mas correm o risco de afetar os valores coletivos e a integridade da democracia em geral. O simples fato de saber que a infraestrutura existe, mas não ser capaz de determinar se está atualmente a ser utilizada, pode levar a graves efeitos inibidores no exercício de direitos políticos, como a liberdade de expressão e a liberdade de associação.

É importante observar, contudo, que tais críticas se dirigem à redação da Proposta de Regulamento feito pela Comissão Europeia, que referenciava as infrações penais contidas no artigo 2.º, n.º 2, da Decisão-Quadro 2002/584/JAI do Conselho, cuja redação é mais abrangente do que a listagem constante no anexo II do texto final do Regulamento. Logo, o Regulamento,

em sua versão final, reduziu consideravelmente os tipos penais justificadores da utilização de identificação biométrica à distância em tempo real.

Nada obstante, a crítica é pontuada, pois reflete, também, a suposta falta de necessidade de uso da tecnologia pela inexistência de urgência (Ebers *et al.*, 2021).

Outra crítica, mais geral à gestão dos sistemas de risco elevado, que também se aplica às hipóteses de uso da identificação biométrica à distância em tempo real, diz respeito ao fato de a avaliação de conformidade ser realizada pelo próprio responsável sem haver, ademais, parâmetros claros do que ser considerado, o que abre margem para a ineficácia do mecanismo (Smuha *et al.*, 2021).

Conforme Smuha *et al.* (2021), a proposta da Comissão Europeia para o Regulamento (que foi em boa medida incorporada no texto final quanto à identificação biométrica) deixa importantes tarefas nas mãos dos responsáveis pelo sistema sem garantia de uma supervisão adequada, o que pode resultar em violações a direitos fundamentais, de modo a se demandar controle independente *ex ante*.

Esse ponto é importante porque a avaliação de impacto de direitos fundamentais, embora não constante na Proposta de Regulamento da Comissão analisada por Smuha *et al.* (2021), é alvo de mera comunicação à autoridade nacional de fiscalização do mercado, conforme artigo 27, item 3, sem previsão de efetiva validação por organismo de supervisão independente (União Europeia, 2024).

As críticas ao Regulamento podem ser resumidas, então, nos seguintes pontos: 1) falta de estudos sobre a efetividade da tecnologia; 2) abertura de margens discricionárias para aplicação pelos Estados, notadamente ante a zona cinzenta do conceito de segurança nacional; 3) falta de regras claras e precisas a potencializar confusões e violações a direitos fundamentais; 4) rol de hipóteses de exceção amplamente largo, sem situações de urgência; 5) desconsideração que, uma vez fixada a infraestrutura da tecnologia, ela tenderá a ser reproduzida, gerando *chilling effect*; e 6) ausência de validação da avaliação de impacto em direitos fundamentais por organismo de supervisão independente.

Passa-se a abordar tais críticas.

Em primeiro lugar, embora seja salutar a existência de estudos sobre o tema, não se visualiza a necessidade de que estes devessem ter sido feitos antes da edição do Regulamento.

É pertinente apontar, inicialmente, que tecnologia já se encontra em uso em diversos países, justificando, portanto, a necessidade de pronta regulamentação. Além disso, a autorização de uso fornecida pelo Regulamento não é autoaplicável, mas depende da edição de legislação interna pelos Estados, oportunidade em que eventuais estudos mais concretos sobre a temática poderão ser realizados.

Aliás, dadas as peculiaridades geográficas e sociais de cada Estado, revela-se mais acertado que os estudos sejam realizados pelos países e não de forma comum em todo o bloco europeu.

De qualquer sorte, embora possa se questionar a falta de estudos conclusivos sobre o grau de eficácia da tecnologia, não se pode esquecer da existência de situações práticas nas quais a tecnologia apresentou resultados positivos. Nessa senda, relembra-se o exemplo da ONG americana Thorn, que, mediante emprego de reconhecimento facial, teria conseguido resgatar mais de 10 mil crianças vítimas de tráfico sexual (Oliveira *et al.*, 2022), ou o fato de que a polícia da Índia indiciou que, em 2018, o uso de tecnologia de reconhecimento facial permitiu a identificação de 3000 crianças desaparecidas em somente 4 dias (Zalnieriute, 2024).

Assim, apesar de sempre poder se buscar maiores estudos, há evidências de que a tecnologia apresenta potenciais positivos para segurança pública, destacando-se, inclusive, a constante evolução tecnológica, a aumentar, cada vez mais, os graus de precisão do sistema.

Portanto, considerando esses pontos, reputa-se que a eventual falta de estudos não se torna indicativo de que o Regulamento esteja em desacordo com direitos fundamentais; em verdade, a necessidade premente de regulação da tecnologia, pelo seu efetivo uso em diversos países, tornava imperiosa a inclusão da matéria de maneira criteriosa, como ocorreu.

Relativamente à suposta exacerbada margem de apreciação nacional, as críticas guardam pertinência no que diz respeito às questões de segurança nacional, que se trata de área não submetida ao Regulamento, mas que, em termos práticos, se confunde com a segurança pública em diversos pontos.

Veja-se que, sobre o procedimento para autorização do uso da tecnologia na segurança pública, a margem nacional é limitada e já há balizas bem definidas no Regulamento, de modo que não há acentuado espaço para discricionariedade. Contudo, ao se permitir que questões afetas à segurança nacional não sejam submetidas aos termos do Regulamento e escapem das balizas ali fixadas, abre-se espaço para eventuais abusos no uso da tecnologia e potenciais

violações a direitos humanos e fundamentais, sob o pretexto de segurança nacional em termos definidos em legislações internas.

Esse ponto é relevante, e a preocupação é justificada.

Assume-se que a exclusão das questões de segurança nacional do âmbito de ingerência da União Europeia ocorreu como forma de se obter consenso, pois, do contrário, os países dificilmente acordariam medidas regulatórias em favor do bloco comunitário para assunto tão sensível e íntimo à soberania interna.

Então, embora se suponha que necessária para obtenção de consenso, a exclusão das questões de segurança nacional se revela problemática para aplicação do Regulamento no que diz respeito à identificação biométrica à distância em tempo real.

Quanto à falta de regras claras e precisas a potencializar confusões e violações a direitos fundamentais, entende-se que o Regulamento fixou balizas precisas e rigorosas para possibilitar o uso da identificação biométrica à distância em tempo real nas situações específicas pré-definidas. Sobre o ponto, reputa-se não haver questões dúbias a gerar confusão ou eventualmente abusos.

Nada obstante, concorda-se que o Regulamento não estipulou obrigações específicas quanto ao desenvolvimento de tais sistemas, que, como visto anteriormente, dependem de cuidados especiais.

O Regulamento focou nas hipóteses de uso e como autorizar tal uso de maneira individualizada, mas, quanto ao desenho, desenvolvimento e monitoramento do sistema, valeu-se das regras gerais fixadas para os sistemas de riscos elevados.

Embora tais regras sejam importantes e pertinentes, elas se mostram genéricas (pois direcionadas a diversas gamas de sistemas de inteligência artificial), motivo pelo qual se reputa que seria mais adequado a estipulação de regras precisas para o ciclo de vida da inteligência artificial em voga, conforme abordado na presente obra.

É claro que os Estados, ao autorizarem o uso da identificação biométrica à distância em tempo real, podem fixar regras específicas sobre o ciclo de vida de tais sistemas, mas isso não é imposto, nem previsto especificamente pelo Regulamento (e inclusive poderia gerar questionamento no âmbito europeu por prever diretrizes mais rígidas, que, do ponto de vista do desenvolvedor, significaria prejudicar a competitividade do produto).

Em semelhante toada, por cair na regra geral dos sistemas de risco elevado, a avaliação de impacto de direitos fundamentais não apresenta peculiaridades quanto à identificação biométrica à distância em tempo real e, mais importante, não se sujeita à validação prévia por organismo de supervisão independente, bastando a mera comunicação.

Isso coloca, como os críticos apontam, poder demasiado na mão dos responsáveis pelo sistema, sem validação prévia por organismo independente, o que se mostraria fundamental no caso da identificação biométrica à distância em tempo real, dado seu demasiado impacto em direitos fundamentais e alto grau de intrusão na privacidade individual, além de potencial de vieses discriminatórios.

Assim, concorda-se com as críticas nos pontos acima mencionados, reputando-se que faltou a fixação de regras específicas para implementação dos sistemas de inteligência artificial destinados à identificação biométrica à distância em tempo real, que apresentam peculiaridades a demandar maiores cuidados no seu desenho, desenvolvimento, treinamento e monitoramento.

Apesar de as hipóteses de uso estarem bem definidas e restritas, com procedimentos rigorosos para autorizar referido uso, carece-se de regras específicas pertinentes ao controle de ciclo de vida da tecnologia em si, que, por ser particular e com alto grau de impacto, demanda cuidados especiais, nos termos já abordados.

Sobre a alegação de que o rol de uso seria demasiadamente extensivo, não se concorda particularmente com tal crítica, uma vez que as hipóteses previstas para uso da tecnologia são, como visto, restritas, envolvendo casos bem delineados, que apresentam gravidade a justificar, em tese, o uso do sistema.

Não se esqueça, ainda, que não apenas os Estados podem limitar tais hipóteses, como cada uso deve ser individualmente autorizado por autoridade judicial, o que se revela ponto positivo do Regulamento (Mobilio, 2022) e, certamente, impede utilização excessiva da tecnologia.

Outrossim, não se visualiza fundamento jurídico a limitar o uso da tecnologia apenas para situações urgentes, relembrando-se que a segurança pública é direito fundamental e humano a exigir ações positivas do Estado, de modo que o emprego de esforços para captura de fugitivos se revela pertinente.

Quanto ao perigo de *chilling effect*, entende-se que o Regulamento esboçou preocupação com essa questão, tanto que previu usos extremamente limitados e procedimentalmente vinculados a autorização judicial específica e individual.

Sob esse prisma, não se concorda com a crítica, porquanto as limitações impostas evitam a existência do referido efeito, na medida em que a tecnologia será usada em situações excepcionais e precedidas de autorização judicial, o que denota que a população inteira não estará sujeita aos efeitos do sistema.

Em suma, reputa-se problemática a exclusão da segurança nacional da disciplina do Regulamento, bem como o fato de que não foram previstas obrigações aos desenvolvedores e implantadores específicas sobre a identificação biométrica à distância em tempo real, cujo ciclo de vida da inteligência artificial requer cuidados particularizados, como evitar vieses, preocupação com grupos demográficos e etários, ponderação do *tradeoff* do *threshold*, necessidade de construção de base de dados de qualidade com observância de peculiaridades da segurança pública e de representatividade de diferentes grupos demográficos etc. Além disso, a mera comunicação da avaliação de impacto em direitos fundamentais não parece ser suficiente a mitigar os riscos da tecnologia, que deveria ser validada por organismo de supervisão independente, inclusive para verificar se o desenho, coleta de dados e treinamento do sistema de inteligência artificial foi realizado de acordo com as diretrizes de direitos humanos e fundamentais incidentes na espécie.

Ao que tudo indica, essas problemáticas decorrem do fato de o uso da tecnologia estar previsto em um Regulamento genérico de inteligência artificial e não ostentar um diploma normativo próprio, de modo que determinadas especificidades que devem permear o tema não sejam abordadas (De Hert e Bouchagiar, 2024).

Nada obstante, o Regulamento apresenta diversos pontos positivos.

Em primeiro lugar, o Regulamento se revela importante para possibilitar o emprego de uma tecnologia relevante para combate à criminalidade, que está sempre avançando em seus métodos (Raposo, 2022).

O Regulamento fornece a base jurídica para uso da tecnologia, o que é importante para retirar incerteza sobre a seara (Urquhart e Miranda, 2021).

Ademais, o Regulamento disciplinou procedimento rígido para uso da tecnologia, com necessidade de prévia autorização judicial individualizada, o que é fator positivo (Mobilio, 2022).

O Regulamento assenta hipóteses restritivas para uso da tecnologia, com procedimento rigoroso e individualizado para possibilitar o uso em cada caso, que deve ser direcionado a alvo

específico, com limitações temporais e geográficas, o que certamente mitiga diversas das críticas tecidas pela doutrina ao emprego da tecnologia.

Assim, apesar das críticas, algumas delas pertinentes como baseado acima, o Regulamento se mostra, em grande medida, adequado e pertinente para finalidade que se propõe, sem prejuízo de que haja eventuais espaços para melhorias e maior segurança jurídica e proteção de direitos fundamentais e humanos, como exposto na presente análise.

Nessa senda, concorda-se com a ponderação de Lynch (2024) transcrita no começo do presente subcapítulo, no sentido de que, atualmente, o Regulamento Europeu se revela a melhor representação de parâmetros robustos para regulação da identificação biométrica à distância em tempo real, embora haja espaço para melhorias.

Como bem assinalou Pereira (2022, p. 864-865):

> 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.

Note-se, inclusive, que o autor aborda a Proposta da Comissão Europeia, que foi aperfeiçoada no texto final do Regulamento, mediante alterações a tornar mais criteriosas as possibilidades de uso; logo, revela-se ainda mais evidente que o Regulamento deve ser visto como uma fonte de inspiração legislativa, pois se trata de legislação robusta que forneceu previsões normativas restritas e específicas, com ponderação dos direitos em jogo, para, em situações excepcionais e individualmente analisadas por autoridade judicial, permitir o uso da identificação biométrica à distância em tempo real.

Em linhas gerais, o Regulamento, apesar de eventuais pontos de melhoria, se mostra atento aos direitos humanos e fundamentais em voga, sem prejuízo de potenciais aperfeiçoamentos ao longo de sua implementação. A fiscalização e o monitoramento se revelam essenciais.

Os pontos falhos do Regulamento, notadamente por se tratar de legislação genérica e não específica da identificação biométrica à distância em tempo real, podem ser abordados em solo nacional por meio de lei específica para a temática.

Em síntese, referidos pontos falhos, embora dignos de nota, não justificam considerar o Regulamento como contrário aos direitos fundamentais e humanos, pois o diploma, de fato, apresentou preocupação com aspectos particularizados do uso da identificação biométrica à distância em tempo real e sua interferência em direitos humanos e fundamentais. Apenas alguns deveres específicos inerentes à gestão do ciclo de vida de tal inteligência artificial, dadas as suas peculiaridades anteriormente estudadas, demandariam previsões normativas particularizadas, o que não acabou ocorrendo, sem prejuízo de que, ao longo da implementação do Regulamento, isso seja corrigido, seja por meio da alteração do Diploma, seja por normativas das legislações domésticas dos países, ou seja mesmo, eventualmente, por atos delegados da Comissão Europeia a partir do paradigma do Novo Quadro Legislativo.

Assentada, então, em essência, a observância dos direitos humanos e fundamentais pelo Regulamento, sem prejuízo dos pontos de melhoria assinalados, analisa-se, em seguida, como referida legislação pode influenciar o debate no cenário nacional, considerando, inclusive, os pontos falhos e as diferentes particularidades entre a fixação de uma legislação transnacional (caso do Regulamento) e a elaboração de legislação interna (caso do Brasil).

5. SITUAÇÃO DO RECONHECIMENTO FACIAL PARA SEGURANÇA PÚBLICA NO BRASIL

Estabelecida a normativa europeia sobre a temática, voltam-se os olhos à situação em território brasileiro.

Desde 2000, prevê-se, no Plano Nacional de Segurança Pública, a utilização de tecnologias na área de segurança pública, com aumento de incentivos a partir de 2012 por meio da previsão em editais de financiamento (Vargas e Ribeiro, 2023). Especificamente quanto ao reconhecimento facial por inteligência artificial, a primeira menção expressa à tecnologia aparece no Plano Nacional de Segurança Pública de 2018 (Vargas e Ribeiro, 2023).

Segundo dados do Instituto Igarapé de 2019, há, desde 2011, 48 casos de utilização de tecnologias de reconhecimento facial no Brasil pelo Poder Público ou parceiros privados, com foco primordial nas áreas de transporte e segurança pública (Santos, 2021)[16].

Nos anos recentes, aumentam-se notícias de emprego da tecnologia em solo nacional, presente, desde 2019, em vinte estados das cinco regiões do país (Costa e Kremer, 2022), sem deixarem de vir atreladas a equívocos no funcionamento do sistema (Melo e Serra, 2022).

Nesse sentido, Melo e Serra (2022) mencionam o caso de uma mulher detida no carnaval de 2019 no Rio de Janeiro por engano pela Polícia Militar, enquanto a procurada já estava presa desde 2015.

Mais preocupante seria a informação decorrente do emprego da tecnologia na festa da "micareta" em Feira de Santana/BA em 2019, quando, dos 903 alertas disparados, apenas 15 pessoas tiveram sua identidade confirmada, revelando índice de falsos positivos superior a 95% (Magalhães e Gomes, 2021; Oliveira *et al.*, 2021).

Embora a cobertura jornalística sobre o tema ainda seja, em grande parte, incipiente, a maior parte das matérias analisadas por Santos (2021) traz pontos críticos ao emprego da tecnologia em solo nacional, com apontamento de problemas sérios, como vigilância em massa e uso abusivo de dados individuais.

Apesar das notícias de falta de precisão da tecnologia, carece-se de pesquisas qualitativas sobre a identificação biométrica à distância no Brasil, impedindo a ponderação, em

16 INSTITUTO IGARAPÉ. Infográfico: reconhecimento facial no Brasil. Disponível em: https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/. Acesso em: 15 dez. 2024.

cenário nacional, dos riscos e benefícios do instrumental para consecução da segurança pública (Magalhães e Gomes, 2021)

A questão se torna mais problemática, na medida em que há pouquíssima informação sobre a forma de implantação e funcionamento dos sistemas, dificultando sua fiscalização (Faria e Silva, 2023).

Inclusive, a implantação de referidos sistemas por entidades alheias à estrutura de segurança pública desperta preocupação.

Em tal senda, Silva *et al.* (2022), ao comentar a implantação do sistema de identificação biométrica à distância em tempo real no metrô de São Paulo, enfatizam a impossibilidade de que as atividades de segurança pública sejam desempenhadas por entidade não inserta na estrutura da segurança pública. Veja-se (Silva *et al.*, 2022, p. 291):

> Não havendo dúvidas sobre a utilização do sistema na política de segurança pública e sabendo que o reconhecimento facial trabalha com a comparação do rosto captado em tempo real com um banco de dados prévio, parece evidente que o corpo funcional do Metrô, ou até mesmo os particulares que estarão operando o sistema, já que nem o edital nem o contrato deixam claro quem operará o sistema após a implantação, terão acesso ao banco de dados da Secretaria de Segurança Pública, pois somente este tem a informação de quem são as pessoas que tem ordem de prisão contra si e também é o principal órgão responsável pela identificação civil da população.
>
> Tal situação fere direitos fundamentais tais como: direito à intimidade, privacidade, imagem do usuário e direito a proteção de dados pessoais, pois tais informações não são de domínio público e sequer podem ser requisitadas por algum interessado, sendo de conhecimento exclusivo dos integrantes do sistema de segurança pública, do Ministério Público e do Poder Judiciário. Patente a ilegalidade e/ou inconstitucionalidade.

Pontuam os autores que, caso a tecnologia seja implantada no sistema de transporte público, o acesso deve ser concedido aos órgãos de investigação estatal, no intuito de que estes possam desempenhar suas atividades, sem liberar acesso a seus bancos de dados sigilosos (Silva *et al.*, 2022).

Por outro lado, também há indícios de usos positivos da tecnologia em solo nacional.

Em pesquisa sobre a identificação biométrica à distância no estado da Bahia, Vargas e Ribeiro (2023, p. 209) indicam a “inexistência de erros quanto ao reconhecimento de pessoas,

até novembro de 2021, quando tinham sido capturadas 282 pessoas foragidas ou procuradas pela Justiça".

Transcreve-se a lição dos autores sobre os pontos positivos encontrados (Vargas e Ribeiro 2023, p. 209-210):

> Outros pontos positivos também chamaram atenção: o cumprimento de direitos fundamentais, a exemplo da não utilização do RF para análise situacional ou comportamental das pessoas; utilização de expansão de mecanismos prévios de participação popular como audiências públicas e envolvimento de órgãos de controle como o TCE-BA, MP-BA e PGE-BA, pelo projeto Vídeo-Polícia Expansão; não compartilhamento de dados sensíveis biométricos com entidades privadas ou transferência internacional; existência de controles de acesso aos dados; cloud (nuvem) privada e preocupação com a segurança do Centro de Controle de Operações onde se localiza o data center com os dados armazenados.
>
> Destaca-se, positivamente ainda, a informação quanto à existência de protocolo interno nas polícias da Bahia limitando a abordagem a pessoas reconhecidas pelo RF com similaridades acima de 90%, o que reduziria chances de erros no RF – o que foi feito mesmo havendo no Termo de Referência da licitação do projeto Vídeo-Polícia Expansão a possibilidade de a abordagem poder ser realizada em caso de similaridades acima de 50%.

Nada obstante, os autores indicam também riscos a direitos fundamentais decorrentes da falta de regulamentação do tema, bem como a falta de consulta à sociedade civil para implantação da tecnologia e a falta de transparência nos dados oficiais (Vargas e Ribeiro, 2023).

Então, mesmo nas hipóteses em que há potencial uso profícuo da tecnologia, ainda se critica a falta de regulamentação e a ausência de transparência, o que caracteriza risco de abusos em prejuízo a direitos fundamentais, com mitigação da possibilidade de fiscalização pela nebulosidade decorrente da falta de balizas claras para emprego da tecnologia.

Em suma, a discussão sobre o tema ainda está em estágio inicial, carecendo-se de regulamentação e fiscalização, de modo a tornar o ambiente propício para potenciais abusos e discriminações (Coimbra *et al.*, 2023).

5.1. VÁCUO NORMATIVO ESPECÍFICO E PROCESSOS LEGISLATIVOS EM TRÂMITE

Em âmbito federal, o uso de tecnologias de reconhecimento facial na segurança pública é incentivado desde, pelo menos, 2019, por meio da Portaria n. 793/2019 do Ministério da Justiça, que permite o uso de recursos do Fundo Nacional de Segurança Pública para tal finalidade (Daguer *et al.*, 2022).

Dentre as ações destinadas para o "Eixo Enfrentamento à Criminalidade Violenta", encontra-se "fomento à implantação de sistemas de videomonitoramento com soluções de reconhecimento facial, por Optical Character Recognition – OCR, uso de inteligência artificial ou outros*",* vide artigo 4º, §1º, III, alínea "b", da referida Portaria, hoje já revogada (Brasil, 2019c, cap. II, artigo 4º, §1º, III, alínea "b").

Acontece que, como assinalado, apesar de a tecnologia já estar em uso em solo nacional, resultando, inclusive, em abordagens policiais, não há qualquer normativa específica.

Mesmo a Lei Geral de Proteção de Dados, Lei n. 13.709/2018, não se aplica à área de segurança pública, por força do art. 4º, III, "a" e "d", do referido diploma normativo (Oliveira *et al.*, 2022).

Para suprir a lacuna da LGPD na seara de segurança pública, existem o Anteprojeto de Lei de Proteção de Dados Pessoais para Segurança Pública e Persecução Penal, oriundo de proposta apresentada por comissão de juristas e conhecido como "LGPD Penal", e o Projeto de Lei nº 1.515/2022, apresentado pelo então deputado Coronel Armando (Azevedo *et al.*, 2022).

Quanto ao reconhecimento facial, o Anteprojeto de LGPD Penal regularia o tema, segundo Santos (2021), entre os artigos 42 e 44.

Analisando mencionado texto[17], percebe-se que tais artigos se encontram no Capítulo VII, sobre "TECNOLOGIAS DE MONITORAMENTO E TRATAMENTO DE DADOS DE ELEVADO RISCO" (Brasil, 2019a, cap. VII).

Embora não haja qualquer menção expressa a reconhecimento facial ou identificação biométrica à distância, a referida autora conclui que referidas tecnologias estão englobadas na mencionada disposição por se tratar de tecnologia de monitoramento e de tratamento de dados de elevado risco (Santos, 2021). Em semelhante conclusão, alinham-se Azevedo *et al.* (2022).

---

17 BRASIL. Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal. Elaborado pela Comissão de Juristas instituída por Ato do Presidente da Câmara dos Deputados. Disponível em: https://static.poder360.com.br/2020/11/DADOS-Anteprojeto-comissao-protecao-dados-seguranca-persecucao-FINAL.pdf. Acesso em: 06 out. 2024.

Para implantação da tecnologia, conforme o Anteprojeto necessita-se de: 1) previsão legal específica; 2) análise do impacto regulatório; 3) Relatório de Impacto à Proteção de Dados Pessoais (Azevedo *et al.*, 2022).

O Relatório de Impacto à Proteção de Dados Pessoais está previsto no artigo 13, parágrafo único, do Anteprojeto, no sentido de que a "autoridade competente responsável pelo tratamento de dados pessoais sensíveis elaborará relatório de impacto à proteção de dados pessoais e informará o Conselho Nacional de Justiça*"* (Brasil, 2019a, cap. II, seção II, artigo 13, parágrafo único).

Ademais, necessita-se de relatório de impacto de vigilância, composto por uma avaliação de risco (Santos, 2021).

Os riscos do sistema, por sua vez, são definidos a partir da natureza dos dados, da finalidade específica do tratamento e da possibilidade de gerar tratamento discriminatório (Azevedo *et al.*, 2022).

O artigo 43, demonstrando intenção de regular identificação biométrica à distância, veda o uso de "tecnologias de vigilância diretamente acrescida de técnicas de identificação de pessoas indeterminadas em tempo real e de forma contínua quando não houver a conexão com a atividade de persecução penal individualizada e autorizada por lei e decisão judicial" (Brasil, 2019a, cap. VII, artigo 43).

Percebe-se, nessa senda, que o modelo, em certa medida, seguiu a previsão do Regulamento Europeu, no sentido de que a autorização para uso da tecnologia seria individualizada e dependente de decisão judicial.

É digno de nota, ainda, que o artigo 44 do referido Anteprojeto estipulou que o "Conselho Nacional de Justiça emitirá opiniões técnicas ou recomendações referentes à utilização de tecnologias de vigilância ou o tratamento de dados pessoais que representem elevado risco para direitos, liberdades e garantias dos titulares dos dados*"*, inclusive com possibilidade de realização de auditoria em caso de denúncia sobre o sistema, conforme §2º do artigo 44 (Brasil, 2019a, cap. VII, artigo 44).

Isso demonstra a submissão do uso da tecnologia a órgão independente e com autonomia (Azevedo *et al.*, 2022).

O Projeto de Lei nº 1.515/2022, por sua vez, apesar de apresentar objetivos similares ao Anteprojeto, de modo a, teoricamente, inclui-lo no processo legislativo, apresentou, em seu cerne, propostas distintas (Azevedo *et al.*, 2022).

Inclusive, o regulamento atinente a tecnologias de monitoramento foi retirado do referido Projeto de Lei, havendo apenas a exceção de a autoridade supervisora (que, no Projeto de Lei, é a ANPD), solicitar relatório de impacto às autoridades competentes (Azevedo *et al.*, 2022).

Azevedo *et al.* (2022, p. 22) concluem pela inadequação do referido Projeto de Lei para proteção de dados pessoais, assentando o seguinte sobre a questão das tecnologias de monitoramento:

> Com isso, o PL cria uma permissão irrestrita para o tratamento de dados pessoais por meio de tecnologias de monitoramento, prática entendida como de alto risco aos direitos fundamentais e liberdades individuais dos titulares de dados. Assim, vai na contramão da tendência global de regular esses riscos, ignorando todo o conhecimento já produzido sobre os potenciais efeitos deletérios produzidos através do uso desregulado dessas tecnologias.

Outro ponto relevante diz respeito ao fato de que mencionadas propostas direcionam-se à proteção de dados pessoais, pouco abordando (ou nada) o tema da inteligência artificial, que, como visto ao longo do presente trabalho, demanda cuidados específicos em razão de suas peculiaridades, sobretudo ao se trata de identificação biométrica à distância em tempo real.

Portanto, referidas propostas são insuficientes à regulação do tema, ficando aquém de todas as especificidades que revolvem a tecnologia, embora, quanto ao Anteprojeto, revele-se elogiável em alguns pontos, como a necessidade de decisão judicial (à semelhança do Regulamento Europeu), dependência de prévia legislação específica (em que poderia se aclarar pontos pertinentes à tecnologia) e de relatório de impacto de vigilância, e a previsão de órgão de fiscalização independente e autônomo.

Além dessas propostas relativas ao tratamento de dados na área da segurança pública, há os seguintes projetos de lei que tramitam no Congresso Nacional sobre a regulação da inteligência artificial: os Projetos de Lei n. 2338 de 2023 de autoria do Senador Rodrigo Pacheco (PSD/MG), n. 4.612 de 2019, n. 9.736/2018 (Magalhães e Gomes, 2021; Daguer *et al.*, 2022), n. 21/2020 (Costa e Kremer, 2022), e n. 759/23.

O Projeto de Lei n. 9.736/2018 se limita a acrescentar na Lei n. 7.210/1984, a Lei de Execução Penal, o artigo 107-A, com a seguinte redação: “As informações constantes da guia de recolhimento serão complementadas pela identificação biométrica por reconhecimento facial, quando o custodiado for recolhido a um estabelecimento penal” (Brasil, 2018a, artigo 2º).

É evidente que tal proposta carece do aprofundamento necessário para abordar o reconhecimento facial, de acordo com as diversas colocações já tecidas no presente trabalho.

De qualquer sorte, ao se analisar a justificativa do Projeto, percebe-se que a intenção se dirige à verificação da identidade individual do preso, o que diz respeito ao processo de verificação e não de identificação, nem se assemelha a identificação biométrica à distância em tempo real, motivo pelo qual seu objeto é distinto do presente trabalho. Por conta disso, inclusive, não seria necessário o mesmo aprofundamento aqui tecido.

O Projeto de Lei n. 4.612/2019 destina-se a abordar o “desenvolvimento, aplicação e uso de tecnologias de reconhecimento facial e emocional, bem como outras tecnologias digitais voltadas à identificação de indivíduos e à predição ou análise de comportamentos*”* (Brasil, 2019b, cap. I, artigo 1º).

Como se vê, o objeto vai além da mera identificação biométrica, para abranger tecnologias de reconhecimento emocional e com finalidade preditiva, o que está além do escopo do presente trabalho.

A análise se limitará aos pontos que dizem respeito à identificação biométrica à distância em tempo real.

O art. 2º enumera pressupostos, dentre os quais se incluem vedação a tratamento discriminatório (inciso I), proibição de vigilância massiva (inciso II), acesso à informação e ao conhecimento (incido IV), livre iniciativa e concorrência (inciso V) e definição multissetorial de boas práticas e padrões técnicos, éticos, de segurança garantidores dos direitos dos cidadãos (inciso IX) (Brasil, 2019b).

Estipula-se que a face constitui dado biométrico sensível (Brasil, 2019b, cap. II, artigo 3º), como, aliás, já se estipula na LGPD, a atribuir-se competência à Autoridade Nacional de Proteção de Dados (artigo 4º), incluindo a regulamentação de dispositivos da Lei (inciso III) e a decisão final na esfera administrativa cobre interpretação da Lei (inciso V) (Brasil, 2019b).

Seguem-se artigos sobre obrigações dos desenvolvedores e usuários (artigos 5º e 6º), direito aos cidadãos afetados (artigos 7º e 8º), compartilhamento de dados (artigo 9º), segurança e boas práticas (artigos 10 e 11), banco de dados (artigo 12) e disposições finais (artigo 13) (Brasil, 2019b).

Referido Projeto se vale de conceitos genéricos, sem definir em quais casos e de qual forma será possível a identificação biométrica à distância em tempo real (Brasil, 2019b). Ao que aparenta, deixa-se a potencial regulamentação para nível infralegal, abrindo margem para utilização abusiva da tecnologia, em descompasso com as considerações tecidas ao longo do presente trabalho.

Portanto, tal Projeto se mostra insuficiente para regulação do tema, valendo-se de expressões genéricas, carentes de concretude, sobretudo ante as diversas problemáticas despertadas pela identificação biométrica à distância em tempo real.

Outro Projeto de Lei insuficiente é o n. 759/23, destinado a regulamentar os sistemas de Inteligência Artificial, mas que conta com 7 artigos, havendo definição de princípios (artigo 2º) e diretrizes (artigo 3º), além de remeter ao Poder Executivo a elaboração de Política Nacional de Inteligência Artificial (artigo 5º) (Brasil, 2023a).

Inclusive, mencionado Projeto não tem qualquer referência a "reconhecimento facial" ou "identificação biométrica", demonstrando não regular o tema de qualquer forma, a não ser por via indireta mediante previsões genéricas sobre inteligência artificial, o que, claramente, não satisfaz a necessidade de tutela dos direitos em jogo (Brasil, 2023a).

O Projeto de Lei n. 21/2020, que "estabelece princípios, direitos e deveres para o uso de inteligência artificial no Brasil*",* segue os ares genéricos do Projeto de Lei n. 759/23, ao contar com 16 artigos, embora detenha um grau maior de detalhamento ao prever, por exemplo, relatórios de impacto no artigo 13 (Brasil, 2020).

De qualquer sorte, tal Projeto também se baseia em previsões genéricas, não contendo qualquer menção específica a "reconhecimento facial" ou "identificação biométrica" (Brasil, 2020), de modo que é igualmente insuficiente.

Por fim, pode-se considerar que o Projeto de Lei n. 2.338 de 2023 é o mais avançado sobre a temática (Brasil, 2023b).

De início, já se verifica que mencionado Projeto segue o Regulamento Europeu ao categorizar a inteligência artificial a partir dos riscos criados pelo seu uso (Brasil, 2023b).

Sobre a identificação biométrica à distância, ela se encontra listada nas atividades de risco excessivo (vedadas, portanto), mas com autorização para determinados casos. Em tal toada, impõe-se transcrever o artigo 15 de mencionado texto (Brasil, 2023b, cap. III, seção II, artigos 15 e 16):

> Art. 15. 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.
>
> Parágrafo único. A lei a que se refere o caput preverá medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal e o controle judicial, bem como os princípios e direitos previstos nesta Lei, especialmente a garantia contra a discriminação e a necessidade de revisão da inferência algorítmica pelo agente público responsável, antes da tomada de qualquer ação em face da pessoa identificada.
>
> Art. 16. Caberá à autoridade competente regulamentar os sistemas de inteligência artificial de risco excessivo.

Além disso, listaram-se no artigo 17, X, os sistemas biométricos de identificação como de alto risco (Brasil, 2023b).

Percebe-se, então, que referido Projeto de Lei seguiu, de maneira geral, a linha do Regulamento Europeu, relegando a lei específica a regulamentação pormenorizada do tema para possibilitar o uso da tecnologia.

Ao seguir a linha do Regulamento, repisam-se as mesmas considerações tecidas no capítulo anterior desta obra.

Outrossim, é interessante observar que, enquanto para o Regulamento Europeu fazia sentido a remissão a lei específica para uso da tecnologia, porquanto essa deve ser editada pelos países, no intuito de adequar a tecnologia às previsões domésticas, não se vê motivo para tal previsão em Projeto de Lei brasileiro, na medida em que, em tal quadrante, o Poder Legislativo

estaria, a rigor, editando diploma normativo sem eficácia direta, dependendo de outro dele próprio, Poder Legislativo.

Nesse contexto, a previsão se torna verdadeiramente inócua, pois, ao depender de outra Lei pelo próprio Poder Legislativo federal, a matéria será novamente apreciada e com ampla possibilidade de alteração, o que revela que as disposições teriam caráter meramente simbólico, mas despidas de verdadeira normatividade.

Além disso, o Projeto de Lei, em sua redação originária, está mais aquém em termos de especificidade quanto à identificação biométrica à distância em tempo real do que o Regulamento Europeu.

Não passa despercebido, por oportuno, que há diversas emendas ao Projeto (144 até 08 de outubro de 2024, salvo melhor juízo – Brasil, 2023b), o que demonstra as intensas tratativas sobre o tema.

Por meio desse apanhado dos processos legislativos que tramitam sobre a matéria, é possível se situar na abordagem da temática no Brasil e, assim, traçar parâmetros para elaboração de um diploma sobre identificação biométrica à distância em tempo real condizente com a proteção de direitos fundamentais e humanos.

Antes disso, mostra-se pertinente esclarecer a relevância do estudo do Regulamento Europeu para tal finalidade.

5.2. RELEVÂNCIA DO REGULAMENTO EUROPEU (EFEITO BRUXELAS)

Já referenciado anteriormente, o Efeito Bruxelas pode ser compreendido como o fenômeno decorrente da influência da legislação europeia em relação a outros agentes estatais e não estatais fora do mencionado bloco econômico (Sousa *et al.*, 2024).

Essa influência não ocorre apenas pelo tamanho do mercado europeu, mas também em razão da arquitetura institucional europeia (Bradford, 2020).

Segundo Rodrigues (2021, p. 205), trata-se da:

> [...] habilidade unilateral da União Europeia (UE) de regular o mercado global, levando normas e regulações unilaterais do bloco comunitário para países

> terceiros por meio de atores privados apoiando-se na expressividade de seu mercado interno.

O Efeito Bruxelas revolve a capacidade de as normativas europeias influenciarem o mercado global, afetando tanto as condutas dos agentes econômicos, quanto as legislações internas dos países.

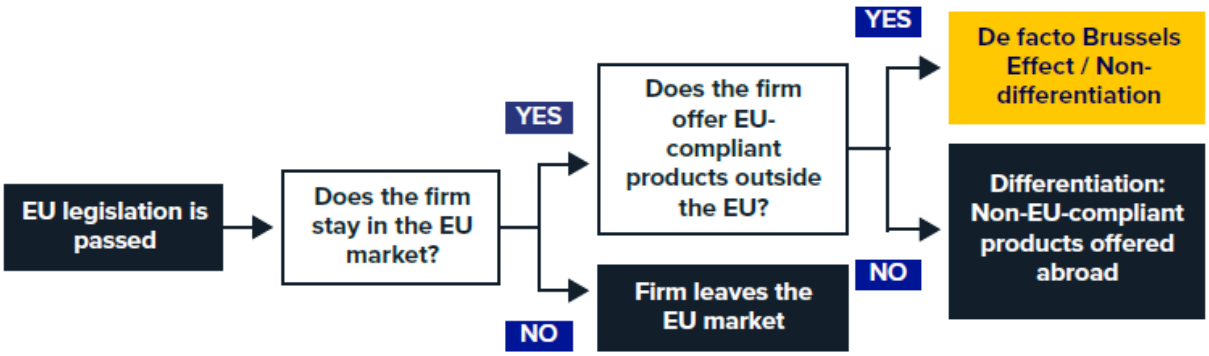
O referido Efeito pode ser subdividido em *de facto* e *de jure* (Bueno e Canaan, 2024).

O Efeito Bruxelas ocorre *de facto* quando as empresas voluntariamente aderem aos regulamentos europeus e passam a replicar produtos harmonizados em ordenamentos estrangeiros, sem tais exigências (Siegmann e Anderljung, 2022).

Isso ocorre porque, ao aderir à regulamentação europeia, a empresa se vê diante de um dilema quanto aos produtos comercializados em outros mercados: diferenciá-los dos vendidos no mercado europeu ou reproduzir as mesmas exigências europeias mesmo que não haja tal imposição em outros mercados. Em tal contexto, o efeito *de facto* acontece quando a empresa opta por não diferenciar os produtos, passando a replicar o padrão harmonizado europeu em outros mercados (Siegmann e Anderljung, 2022).

A figura abaixo demonstra a árvore de decisão do Efeito Bruxelas *de facto*:

Figura 9 – árvore de decisão do Efeito Bruxelas *de facto*



Fonte: Extraído de Siegmann e Anderljung, (2022, p. 19).

Percebe-se, então, que o Efeito Bruxelas *de facto* decorre de decisões dos agentes privados e não advém de qualquer normatividade imposta pelas nações estrangeiras. Decorre,

pois, da dinâmica dos mercados, em que as companhias transnacionais aderem voluntariamente aos padrões criados pela União Europeia e os replicam globalmente (Bueno e Canaan, 2024).

São cinco fatores que levam aos efeitos *de facto*: 1) características do mercado favoráveis decorrentes do tamanho do mercado europeu; 2) maior severidade, ainda que em parte, das normativas europeias em relação a outras; 3) capacidade regulatória aguçada da União Europeia em produzir legislações robustas e claras, a diminuir custos regulatórios e aumentar a probabilidade de aderência pelas empresas, atrelada à valorização de produtos conformes pelos consumidores; 4) inelasticidade relativa da oferta e da demanda dentro e fora da União Europeia, de modo a não alterar o tamanho do mercado em razão da regulamentação; e 5) custos de diferenciação, de modo que as empresas, ao optarem por aderir ao regulamento europeu, incorreriam em custos para diferenciar dois tipos de produtos: um conforme, comercializado no âmbito europeu, e um não conforme, a ser comercializado no resto do globo (Siegmann e Anderljung, 2022).

Por sua vez, o Efeito Bruxelas *de jure* acontece quando são adotadas por governos estrangeiros normativas semelhantes às estabelecidas em âmbito europeu (Bueno e Canaan, 2024).

Siegmann e Anderljung (2022) concebem quatro meios a partir do qual o efeito *de jure* pode ocorrer.

Em um primeiro exemplo, tem o que os autores chamam de *Blueprint Adoption*, consistente na replicação da legislação europeia por Estados estrangeiros, sob a crença de que os dispositivos europeus serão capazes de alcançar os objetivos regulatórios (Siegmann e Anderljung, 2022).

Além disso, há a possibilidade de negociações multilaterais e bilaterais em que podem ser promovidos os padrões europeus, com destaque para a padronização realizada, por exemplo, pela ISO (Siegmann e Anderljung, 2022).

Uma terceira hipótese consiste no lobby realizado por empresas em razão do Efeito Bruxelas *de facto*, uma vez que, ao adotarem os padrões europeus de conformidade, as multinacionais podem ficar em desvantagem concorrencial com empresas que não adotam tais padrões, justificando, então, que promovam a tentativa de uniformizar a legislação internacional aos padrões europeus.

Por fim, caso haja extraterritorialidade dos requisitos europeus de transação, isso pode acarretar pressão econômica em outras nações para adotar normativas semelhantes (Siegmann e Anderljung, 2022).

Um exemplo do Efeito Bruxelas diz respeito ao Regulamento Geral de Proteção de Dados de 2016 (Bueno e Canaan, 2024).

Referido Regulamento apresentou tanto efeitos *de facto* quanto *de jure*.

Sob o prisma *de facto*, os padrões do Regulamento Geral de Proteção de Dados foram reconhecidos como globalmente aceitos pelas empresas, dada a importância do mercado europeu, bem como em razão da inelasticidade que envolve a natureza dos dados pessoais (Bueno e Canaan, 2024).

Relativamente ao aspecto *de jure*, o Regulamento Europeu provocou a revisão de regulações de outros países para se adequar às normativas europeias (Bueno e Canaan, 2024).

No Brasil, é notória a influência do Regulamento Europeu na Lei Geral de Proteção de Dados, Lei n. 13.709/2018 (Brasil, 2018b).

Com efeito, conforme Lorenzon (2021, p. 50), há

> [...] grandes similaridades entre ambas as normas, como a obrigação de provedores de serviço e conteúdo terem um Encarregado de Proteção de Dados, o estabelecimento de uma agência reguladora nacional, e os detalhamentos das multas, o que é compreensível visto que a GDPR serviu de inspiração para a elaboração da LGPD.

Logo, a ocorrência do Efeito Bruxelas em solo nacional não é novidade.

Sobre o Regulamento Europeu de Inteligência Artificial, Siegmann e Anderljung (2022) entendem que pode ocorrer o Efeito Bruxelas *de facto* sobre partes da normativa, incluindo, nessa perspectiva, a identificação biométrica à distância.

Isso porque, segundo os autores, os padrões europeus podem ser percebidos como os marcos ideais nessas aplicações controversas, em que existe grande pressão por determinados grupos para banimento do uso (Siegmann e Anderljung, 2022). Logo, as empresas multinacionais, ao adotar os padrões europeus para uso da tecnologia, poderiam buscar se isentar de questionamento em outros países, até porque algumas delas já haviam se proposto a cessar o uso da tecnologia (Siegmann e Anderljung, 2022).

Também há espaço para Efeito Bruxelas *de jure* no que diz respeito à identificação biométrica à distância em tempo real, o que pode ser o impacto mais significativo do Regulamento (Siegmann e Anderljung, 2022).

Como se vê, no Brasil, ante o trâmite do Projeto de Lei n. 2.338 de 2023 (Brasil, 2023b), que se trata do mais avançado sobre a matéria, já se percebe a ocorrência do Efeito Bruxelas sob o prisma *de jure*.

Mencionado Projeto de Lei replica a estrutura normativa do Regulamento Europeu e, sobre o objeto do presente estudo, adota disposições semelhantes.

Exatamente por isso, portanto, se revelou importante e fundamental o estudo e aprofundamento do Regulamento Europeu de Inteligência Artificial.

Não passa despercebida, todavia, a existência de escolhas diversas quanto à regulamentação do tema por países como China, Rússia e Estados Unidos da América (Raposo, 2022; Lynch, 2024; De Hert e Bouchagiar, 2024), notadamente mais permissivos quanto ao uso da tecnologia. Isso certamente acarretará o desenvolvimento mais acelerado de tecnologias em tais países, o que, diante da tendência de maior unificação das normas penais em razão do fenômeno da globalização (Moraes, 2016), pode impactar o uso da tecnologia em solo nacional.

Sobre o tema, aliás, a regulação excessiva ante a existência de territórios mais permissivos ao desenvolvimento de referidas tecnologias pode acarretar competição desleal entre regiões e eventual atraso tecnológico local, conforme preocupação bem exposta por Moraes e Lisboa (2024, p. 28):

> A ausência de uma regulamentação harmonizada a nível mundial pode, de fato, resultar em uma competição desleal entre regiões que adotam padrões rigorosos e aquelas que operam sem restrições similares. Isso cria um cenário em que produtos e serviços estrangeiros não regulamentados têm vantagens competitivas, especialmente em áreas sensíveis como a medicina, onde a inovação tecnológica é crucial. O atraso no desenvolvimento científico no Ocidente, causado pela sobrecarga regulatória, é uma preocupação legítima. No entanto, essa preocupação deve ser equilibrada com a necessidade de proteger a saúde pública e os direitos humanos.

Ademais, a globalização traz também novas formas de criminalidade, de índole transnacional (Moraes, 2016), de modo que a ocorrência de crimes transnacionais trará questões relevantes acerca da aplicação da tecnologia em ordenamentos jurídicos diversos.

Sobre o tema, impõe destacar que cooperações internacionais têm a capacidade de gerar ciclo virtuoso em prol da persecução criminal, como bem destacado em estudo de Bechara, Smanio e Girardi (2019), de modo que muitos entraves regulatórios em solo nacional podem gerar eventuais barreiras à cooperação em matéria da presente tecnologia.

De qualquer sorte, apesar dessas potenciais controvérsias futuras, reputa-se que, no atual estágio normativo brasileiro, a Regulamentação Europeia, seja pela tradição pátria em endossar o pensamento jurídico europeu, seja pelo efeito Bruxelas, mostra-se normativa bastante relevante a influenciar o debate nacional sobre o tema.

Presentes, então, todos os tópicos estudados, passa-se a analisar como os pontos abordados podem levar à construção de uma normativa em solo nacional condizente com a proteção de direitos fundamentais e humanos, tomando por base o Regulamento Europeu.

5.3. COMPATIBILIDADE DO REGULAMENTO EUROPEU COM O ORDENAMENTO BRASILEIRO E A TUTELA DOS DIREITOS HUMANOS

Como visto em tópico anterior, o Regulamento Europeu apresenta peculiaridades que não são diretamente aplicáveis em solo nacional.

Em primeiro lugar, trata-se de dispositivo transnacional que não busca exaurir o tema, deixando aos países margem para disciplinar o procedimento referente ao uso da tecnologia, embora seja restrito quanto às possibilidades e às balizas de uso, além de firmar certos pré-requisitos a serem observados no procedimento a ser criado.

Exatamente por não ser exauriente, o Regulamento deixa lacunas, que não teriam motivos para existir em legislação brasileira sobre o tema.

Outrossim, foi assentado que o Regulamento não se aplica a atividades militares, de defesa ou de segurança nacional, o que permite, em tese, o uso da tecnologia em voga para tais finalidades sem cumprimento das normativas mencionadas.

Embora Azevedo *et al.* (2022) reputem que as atividades de defesa e segurança nacionais ostentem particularidades a justificar a separação em relação às previsões normativas

sobre segurança pública[18], no entender deste trabalho, a exclusão de mencionadas finalidades, pelo menos para a identificação biométrica à distância em tempo real, oferece sensíveis riscos.

Isso porque, uma vez instalado o aparato e em funcionamento a tecnologia, a permissão de uso abrangente para determinada finalidade pode resvalar nos abusos já estudados nesta pesquisa, até porque, no dia a dia, a diferenciação se a tecnologia está sendo empregada para escanear faces para fins de segurança pública ou segurança nacional perde relevo.

Com efeito, uma vez em funcionamento, a tecnologia estará reiteradamente escaneando rostos da população e ocasionando os riscos mencionados anteriormente, de modo que, ainda que a finalidade seja restrita (isto é, atividades militares, de defesa ou de segurança nacional), o potencial lesivo à população ainda é grande caso tal atividade careça de qualquer regulamentação.

Inclusive, importa rememorar o caso Glukhin v. Rússia, julgado pela Corte Europeia de Direitos Humanos (Lynch, 2024), que revolvia o protesto individual de um cidadão contra o governo, que, a depender da linha argumentativa, poderia se buscar o enquadramento como questão de segurança nacional (até porque, como visto, os limites da matéria não são bem definidos), a reforçar o perigo de tais exceções à incidência da regulação.

Embora não se negue que atividades militares, de defesa e de segurança nacional detenham particularidades, as características da tecnologia da identificação biométrica à distância em tempo real recomendam cautela na exclusão de determinadas finalidades, na medida em que mesmo restritas permissões, se não reguladas de forma devida, podem resultar em abusos.

Assim, compreendendo que, no Brasil, o diploma a ser editado é de âmbito nacional e não internacional (não resultando, portanto, em eventuais impasses diplomáticos ou discussões

---

18 Se não, veja-se o que os autores dizem sobre a inclusão no PL 1515/2020 de atividades de defesa e de segurança nacionais, em comparação com o Anteprojeto da LGPD Penal (Azevedo e outros, 2022, p. 07): “A restrição de escopo feita pelo APL tem uma razão de ser: as atividades de segurança do Estado e de defesa nacional são significativamente diferentes das atividades de segurança pública e persecução penal. Grosso modo, enquanto os conceitos de segurança do Estado e defesa nacional se relacionam com a proteção do Estado brasileiro contra ameaças internas e externas, os conceitos de segurança pública e persecução penal tratam da proteção – de forma preventiva e repressiva – a bem jurídicos tutelados pela legislação penal.
O escopo amplo estabelecido no PL é tecnicamente questionável, uma vez que tanto a atividade de segurança do Estado como a de defesa nacional possuem fundamentos, finalidades, regulações e ecossistemas institucionais incompatíveis com o desenho legal concebido no APL, e reproduzido parcialmente no PL. Assim, as inovações propostas para acomodar essas duas atividades não são capazes de oferecer níveis de controle proporcionais aos riscos, impactos sociais, econômicos e políticos gerados. Como veremos, no decorrer do texto do PL há várias incongruências quando o tema é segurança do Estado e defesa nacional”.

acerca de soberania), sugere-se a inclusão de regulação, ainda que particular, para uso da tecnologia direcionada a atividades militares, de defesa e de segurança nacional.

A regulamentação para atividades militares, de defesa e de segurança nacional não necessita ser idêntica àquela formulada para segurança pública, mas deve haver algum tipo de regulamentação normativa, sob pena de incidência dos riscos apontados na presente pesquisa.

Assentado tal ponto, reputa-se que, em geral, o Regulamento Europeu se cuida de boa inspiração normativa para regulamentação do tema em sede nacional.

Como visto, a elaboração de disciplina normativa específica para a identificação biométrica à distância em tempo real (ainda que, eventualmente, constante em diploma mais genérico) deve levar em consideração, sob o ponto de vista técnico, a inexistência de neutralidade da tecnologia, o *trade-off threshold* (falsos positivos/falsos negativos), qualidade de dados (banco de dados), vieses (erro algorítmico e localização das câmeras), a necessidade de supervisão humana, e, sob o ponto de vista jurídico, as seguintes interferências: autonomia/privacidade (qualidade de dados e consenso), direitos à liberdade de expressão e à reunião (*chilling effect*), discriminação, princípio da presunção de inocência, princípios da transparência e da explicabilidade, grupos etários (crianças e idosos).

O Regulamento Europeu buscou equacionar os riscos e o potencial benefício da tecnologia.

De início, as hipóteses restritas para uso, reservada a situações de maior gravidade, já revelam acerto da normativa ao não deixar margens amplas que podem resvalar para abusos ou arbítrios.

Ainda, o rol legal restrito é fator importante para não criar receio coletivo no uso de espaços públicos, pois a limitação do uso da tecnologia cria confiança no indivíduo de que não será rastreado por motivos insignificantes ou obscuros.

Soma-se a isso que o mero preenchimento de uma das exceções legais não é suficiente para uso da tecnologia. Devem ser cumpridas balizas rígidas e seguir procedimento rigoroso.

A cada utilização individual, o Regulamento Europeu impõe a realização de ponderação particularizada, no intuito de determinar se, para aquela situação específica, o uso da tecnologia é proporcional.

Não bastasse a ponderação individualizada, a ser exercida por magistrado (ou autoridade administrativa com decisão definitiva), o sistema também deve passar por uma avaliação global

de impacto sobre os direitos fundamentais, analisando de forma ampla como pode afetar os direitos da população.

Logo, são dois mecanismos a garantir que a tecnologia, mesmo nos casos restritos de uso, não resulte em abusos ou situações violadoras de direitos fundamentais.

O procedimento, por sua vez, abrange a concessão de ordem judicial individualizada para cada uso, em que se limita "ao estritamente necessário no que diz respeito ao período de tempo e ao âmbito geográfico e pessoal" (União Europeia, 2024, p. 52).

A ordem judicial depende, outrossim, de elementos probatórios mínimos justificadores da utilização do sistema, revelando a inviabilidade de autorização de uso com base em suspeitas abstratas ou afirmações genéricas. Depende-se de dados objetivos ou indícios claros justificantes da utilização do sistema.

Além desses elementos específicos, a tecnologia também se sujeita aos requisitos gerais de sistemas de inteligência artificial de alto risco.

Assim, deve observar, dentre outros, os seguintes dispositivos: Implementação de gestão de risco (artigo 9º); Governança de dados (artigo 10); Elaboração de documentação técnica (artigo 11); Manutenção de registros (artigo 12); Transparência e informação pelos desenvolvedores aos implantadores (artigo 13); Supervisão humana (artigo 14); Exatidão, solidez e cibersegurança (artigo 15) (União Europeia, 2024).

Ademais, sujeita-se à autoridade nacional de fiscalização, com necessidade de registro perante a Comissão Europeia.

Nesse contexto, as previsões normativas do Regulamento fornecem robusto arcabouço normativo a servir de inspiração ao Brasil.

Nada obstante, existem alguns pontos falhos que podem ser melhorados em solo nacional, até porque, como visto, o Regulamento, tratando-se de diploma internacional editado sob o Novo Quadro Legislativo Europeu, deixa margem para regulamentação e aplicação dos dispositivos aos países, sobretudo quanto à identificação biométrica à distância em tempo real, cujo uso efetivo depende de legislações domésticas a serem editadas pelos países membros.

Como pontos problemáticos assinalados anteriormente, constam os seguintes: a exclusão da segurança nacional da disciplina do Regulamento, o fato de que não foram previstas obrigações aos desenvolvedores e implantadores específicas sobre a identificação biométrica remota em tempo real, cujo ciclo de vida da inteligência artificial demanda cuidados

particularizados, como evitar vieses, preocupação com grupos demográficos e etários, ponderação do *tradeoff* do *threshold*, necessidade de construção de base de dados de qualidade com observância de peculiaridades da segurança pública e de representatividade de diferentes grupos demográficos etc. Além disso, a mera comunicação da avaliação de impacto em direitos fundamentais não parece ser suficiente a mitigar os riscos da tecnologia, que deveria ser validada por organismo de supervisão independente, inclusive para verificar se o desenho, coleta de dados e treinamento do sistema de inteligência artificial foi realizado de acordo com as diretrizes de direitos humanos e fundamentais incidentes na espécie.

A questão da segurança nacional já foi abordada.

A seguir, abordam-se pontos que, no entender do presente trabalho, servem para fornecer disposições normativas atentas às particularidades da tecnologia em voga, aperfeiçoando a disciplina normativa do Regulamento Europeu.

Inclusive, esses esforços devem estar inseridos dentro de um escopo mais amplo, consistente na fixação de uma Política Criminal racional, voltada à tutela de bens transindividuais e capaz de combater a criminalidade de massa, de modo a conjugar modelos eficientes e eficazes de enfrentamento ao crime (Moraes, 2016).

Aqui, deve-se atentar para criação de uma política pública direcionada ao correto emprego da tecnologia, o que corresponderia a um verdadeiro *compliance* criminal.

Segundo Saavedra (2016), os debates sobre *compliance* criminal estão no início, mas o tema revolve a criação de mecanismos para prevenir a ocorrência delitiva, bem como estabelecer, quando da ocorrência de desvios, a cadeia de imputação penal.

Nessa senda, o *compliance* criminal, ao se preocupar com a prevenção de condutas delitivas, vai além do direito penal tradicional, focado na reação à ocorrência do crime (Rotsch, 2012).

Por esse prisma, a estipulação de *compliance* criminal para identificação biométrica significa a adoção de controles rigorosos no uso da tecnologia, voltados à aplicação do mecanismo de forma eficiente e eficaz na consecução de uma Política Criminal racional, nos termos preconizados por Moraes (2016).

Como salientado ao longo do presente trabalho, um dos pontos crucias para o êxito da identificação biométrica à distância em tempo real é a criação de um banco de dados com qualidade e representatividade.

Se, em geral, já é importante aos sistemas de inteligência artificial a construção de banco de dados adequados, por conta do aprendizado pela máquina, isso é ainda mais verdade quando se fala em identificação biométrica à distância em tempo real, pois as imagens constantes no banco de dados é que definirão a precisão do sistema e, consequentemente, a potencialidade de vieses, discriminação e violação de direitos humanos e fundamentais.

Acontece que, a despeito da relevância e da sensibilidade do tópico, não há qualquer disciplina normativa sobre o ponto.

Aliás, como revelado pelo estudo TELEFI (2021), não há uniformidade no território europeu acerca da origem dos bancos de dados utilizados para as tecnologias de reconhecimento facial; eles podem ter tanto origem civil quanto criminal.

Entende-se que, ao regulamentar o tema em solo nacional, é importante abordar o tema (ainda que se deixe para atos infralegais a pormenorização regulatória), uma vez que se trata de questão crucial para a tecnologia e que perpassa as vulnerabilidades e riscos expostos em capítulo anterior.

Assim, pretende-se fornecer substrato para construção normativa atenta a tal ponto.

De início, observa-se já haver, em solo nacional, a Lei da Identificação Civil Nacional, editada sob o n. 13.444/2017, que, nos termos do seu artigo 2º, conjuga a (Brasil, 2017, art. 2º):

> I – a base de dados biométricos da Justiça Eleitoral;
>
> II – a base de dados do Sistema Nacional de Informações de Registro Civil (Sirc), criado pelo Poder Executivo federal, e da Central Nacional de Informações do Registro Civil (CRC Nacional), instituída pelo Conselho Nacional de Justiça, em cumprimento ao disposto no art. 41 da Lei nº 11.977, de 7 de julho de 2009 ;
>
> III – outras informações, não disponíveis no Sirc, contidas em bases de dados da Justiça Eleitoral, dos institutos de identificação dos Estados e do Distrito Federal ou do Instituto Nacional de Identificação, ou disponibilizadas por outros órgãos, conforme definido pelo Comitê Gestor da ICN.

Percebe-se que tal Lei permite a criação de amplo banco de dados com a finalidade de identificação dos indivíduos.

A identificação criminal do indivíduo, no Brasil, só ocorre em situações restritas, até porque, conforme art. 5º, LVIII, da Constituição Federal, o *"*civilmente identificado não será

submetido a identificação criminal, salvo nas hipóteses previstas em lei" (Brasil, 1988, título II, cap. I, artigo 5º, LVIII).

Logo, por força constitucional, a identificação criminal só ocorre em casos excepcionais, atualmente disciplinados no artigo 3º da Lei n. 12.037/09 (Brasil, 2009)[19]. Assim, ainda que haja banco de dados das polícias, a origem das imagens será possivelmente do banco de dados de identificação civil, porquanto a identificação criminal, como visto, é exceção.

Nesse prisma, segundo Oliveira *et al.* (p. 119), a Lei da Identificação Civil Nacional (Lei n. 13.444/17) poderia servir como base do banco de dados a subsidiar as tecnologias de reconhecimento facial para segurança pública.

Todavia, ante a abrangência do banco de dados da referida Lei, que busca englobar toda a população nacional, surgem preocupações quanto à sua utilização para fins de segurança pública, já que a maioria das pessoas ali constantes não terá qualquer envolvimento em atividades criminosas.

Sobre o tema, segue comentário de Faria e Silva (2023, p. 15) quanto à edição de Decretos presidenciais destinados a, no espírito da Lei n. 13.44/17, criar Cadastros Nacionais com dados dos cidadãos:

> Em 2019, dois decretos presidenciais (Decreto 10.046/2019 e Decreto 10.047/2019) possibilitaram a criação de uma grande base unificada e compartilhada de dados pessoais dos cidadãos. Os decretos ilustram os atuais riscos de implementação e normalização de sistemas de vigilância em massa, uma vez que permitem o armazenamento de dados biométricos faciais, associados a diversos outros dados biográficos.

19 Vide: "Art. 3º Embora apresentado documento de identificação, poderá ocorrer identificação criminal quando: I – o documento apresentar rasura ou tiver indício de falsificação; II – o documento apresentado for insuficiente para identificar cabalmente o indiciado; III – o indiciado portar documentos de identidade distintos, com informações conflitantes entre si; IV – a identificação criminal for essencial às investigações policiais, segundo despacho da autoridade judiciária competente, que decidirá de ofício ou mediante representação da autoridade policial, do Ministério Público ou da defesa; V – constar de registros policiais o uso de outros nomes ou diferentes qualificações; VI – o estado de conservação ou a distância temporal ou da localidade da expedição do documento apresentado impossibilite a completa identificação dos caracteres essenciais. Parágrafo único. As cópias dos documentos apresentados deverão ser juntadas aos autos do inquérito, ou outra forma de investigação, ainda que consideradas insuficientes para identificar o indiciado" (Brasil, 2009, artigo 3º).

Nesse contexto, uma saída é limitar os dados que serão inseridos no banco de dados destinado à identificação biométrica, sem englobar a totalidade do banco de dados de identificação civil.

Certamente, pelo avaliado no Projeto TELEFI (2021), não há uniformidade na forma de obtenção e na abrangência do banco de dados direcionado ao reconhecimento facial.

Embora relevantes, as preocupações quanto à eventual abrangência demasiada do banco de dados restam mitigadas pelo fato de que o uso da tecnologia ocorrerá em situações extremamente limitadas, calcada em balizas rigorosas e procedimento rígido.

Nessa senda, o fato de a imagem da pessoa constar no banco de dados não significa que ela estará passível de ser abordada, porquanto isso, no arcabouço proposto, depende de uma série de condicionantes destinadas a limitar o uso da tecnologia.

Por outro lado, a maior abrangência do banco de dados possibilitará melhor treinamento do algoritmo e maior precisão, o que revela um *tradeoff*. Com efeito, o incremento do banco de dados traz preocupações relativas aos direitos de privacidade e personalidade envolvidos nos dados biométricos coletados, mas, ao mesmo tempo, ao se aumentar a base de dados, possibilita-se, em termos técnicos, maior precisão do algoritmo.

O ponto de equilíbrio deverá ser dado com base em considerações tanto jurídicas quanto políticas, a partir da regulamentação a ser realizada pelo Congresso Nacional, na medida em que, como visto, cuida-se, em essência, da administração de risco, cujo cerne carrega uma decisão política (que, todavia, não pode ignorar os limites jurídicos e desdobrar em violação injustificada de direitos humanos e fundamentais).

Portanto, o modelo de banco de dados deve ser alvo da regulação, ainda que detalhes da temática possam ser relegadas a atos infralegais.

Em tal toada, a regulação deve estar atenta ao fato de que a identificação biométrica à distância em tempo real depende de imagens com qualidade e com representatividade.

Assim, mostra-se essencial que a previsão normativa indique que o banco de dados detenha imagens de qualidade e com representatividade, buscando evitar vieses demográficos.

Aliás, como visto, no intuito de garantir a qualidade da imagem para a finalidade pretendida, devem ser observados as peculiaridades dos grupos demográficos, pois, conforme estudos técnicos sobre o tema, padrões de luminosidade, por exemplo, variam de acordo com o tom de pele.

É importante, então, que a estipulação do banco de dados venha acompanhada com previsões normativas que assegurem a qualidade das imagens ali constantes; do contrário, o sistema de inteligência artificial estará passível de erros crassos, que, dada a particularidade da atividade desenvolvida, podem resultar em violações a direitos fundamentais e humanos.

Em suma, na regulação da matéria em solo nacional, deve haver previsão acerca da origem do banco de dados a ser formado e a estipulação de padrões de qualidade, ainda que detalhes normativos sejam relegados a atos infralegais.

Isso garante que exigências mínimas sobre o banco de dados devem ser cumpridas para funcionamento da tecnologia, o que é aspecto fundamental para que seu desempenho seja adequado e não resulte em violações a direitos humanos e fundamentais.

Uma vez estabelecida a base de dados, já se pode buscar o treinamento do sistema, pois a mera construção da base de dados, embora essencial, não é suficiente para a precisão do sistema e eliminação de vieses.

O aprendizado da máquina também depende de treinamentos, que, dadas as peculiaridades da tecnologia em voga, se fazem fundamentais para garantir que o sistema não operará com vieses, sobretudo em prejuízo a determinados grupos demográficos.

Nesse contexto, mostra-se aconselhável que, antes do início do uso efetivo, haja treinamento do sistema em condições determinadas na busca de certos graus de precisão.

No treinamento, será possível avaliar, inclusive, os índices de falsos positivos e de falsos negativos, já que se saberá de antemão quem são as pessoas alvo cujas faces são escaneadas (o que é inviável quando o sistema está operando em situação real).

O treinamento deve se pautar não apenas em uma precisão geral do sistema, mas também em precisões atentas a diferentes grupos demográficos, a fim de se determinar a aptidão do sistema em diferentes rostos, englobando a diversidade existente em solo nacional.

Isso é extremamente relevante, pois pode fornecer justificativa para limitação do uso do sistema; por exemplo, caso haja precisão inadequada para identificação de rostos de crianças ou idosos, essa população pode ser excluída dos usos, evitando, assim, os falsos positivos e eventuais violações a direitos humanos e fundamentais.

Como se percebe, o treinamento rigoroso é uma parte essencial do ciclo de vida da inteligência artificial destinada à identificação biométrica, cuja exigência deve constar na

regulação sobre o tema, ainda que detalhes sobre o treinamento sejam relegadas a instâncias técnicas.

É dizer: entende-se relevante a previsão da necessidade de treinamento e que esse treinamento ocorra para fins de alcançar determinados graus de precisão previamente ao uso, atento a diferentes grupos demográficos (ou seja, com índices de precisão para cada grupo demográfico relevante), sendo certo que detalhes técnicos sobre como realizar o treinamento podem ficar a cargo do órgão de supervisão da tecnologia, que deterá conhecimentos específicos sobre a questão (até porque, tratando-se de tecnologia em constante evolução, os detalhes vão se alterar ao longo do tempo).

Ainda, é interessante que o treinamento ocorra em circunstâncias mais próximas possíveis do uso pretendido, simulando o efetivo funcionamento da tecnologia em condições do mundo real.

Sob esse aspecto, é possível que haja prévia instalação das câmeras destinadas à identificação biométrica, mas, antes do acionamento do sistema, elas sejam testadas com alvos pré-selecionados, que voluntariamente façam parte do treinamento, permitindo verificar se o sistema está logrando realizar as identificações corretas e, em caso negativo, quais percentuais de falsos positivos e falsos negativos.

Percebe-se a relevância desse treinamento já nos locais em que se busca o uso da tecnologia, pois simula circunstâncias reais, inclusive quanto à população demográfica cuja face será escaneada.

Outro ponto relevante do treinamento é que ele fornecerá dados a melhor compreender o sistema, de modo que, quando do uso real, o supervisor humano terá elementos para verificar possíveis equívocos.

Por exemplo, ao saber que a precisão do sistema cai determinado percentual quando a pessoa está com chapéu ou óculos escuros, o supervisor humano, ao ser apresentado uma correspondência positiva com tais características, terá elementos para avaliar, previamente, a possibilidade de um falso positivo.

Assim, o treinamento ostenta importância não apenas para garantir níveis de precisão de forma global e para os grupos demográficos relevantes, como também para fornecer informações relevantes sobre o funcionamento do sistema que auxiliará a supervisão humana no desempenho de suas tarefas.

Outro ponto relevante do sistema, que impacta diretamente seu funcionamento, diz respeito ao grau de similaridade exigido para uma correspondência ser considerada positiva.

Como visto anteriormente, quanto maior o grau de similaridade exigido, maior será o número de falsos negativos; ao se abaixar tal grau, aumentam-se os números de falsos positivos.

Cuida-se de uma decisão, a rigor, política a fixação desse grau, devendo levar em conta os benefícios e malefícios da escolha.

Apesar de política, é certo que a escolha não pode redundar em violações a direitos fundamentais e humanos, pois seria juridicamente vedada.

Entende-se que, ao regular o tema, deve ser previsto que órgão supervisor detenha atribuições para estipular os graus de similaridade a serem empregados no sistema.

Por se tratar de uma decisão política e não meramente técnica, é importante que a fixação de tal ponto também passe sob procedimento que garanta algum grau de democraticidade no padrão eleito.

O órgão supervisor, como será visto à frente, deve conter membros da sociedade civil, exatamente no intuito de colocar o uso da tecnologia sob o crivo também da sociedade, dando, assim, contornos democráticos na gestão do equipamento e evitando os riscos de violações a direitos humanos e fundamentais anteriormente vistos.

Logo, a regulação do tema deve estipular que os graus de similaridade da tecnologia estejam sujeitos a supervisão. Inclusive, tais padrões podem ser alterados ao longo do uso da tecnologia, pois, durante seu monitoramento, pode ser percebida alguma inadequação no grau fixado previamente.

Esse ponto é de extrema relevância e impacta de forma profunda a ocorrência dos falsos positivos.

Relembre-se que há diversas notícias de falsos positivos no Brasil a partir do uso da tecnologia. A despeito disso, sequer se sabe qual grau de similaridade o sistema usava, até porque, em geral, ante a falta de regulação da matéria, a questão ficava relegada ao operador, sem publicidade.

Esse aspecto deve ser trazido à luz e ser disponível para avaliação do sistema, inclusive para fins de controle externo, na medida em que revolve ponto fundamental a impactar diretamente a população afetada.

Cuida-se, aliás, de aspecto essencial da transparência do sistema, pois permite a compreensão de seu funcionamento e a origem das falsas correspondências.

Portanto, é salutar que, na regulação do tema, haja previsão sobre a possibilidade de fixação do grau de similaridade por órgão de supervisão e o controle dos resultados do sistema em vista de referido grau de similaridade.

Isso possibilitará não apenas a escolha política de forma democrática acerca do *tradeoff* adequado para o *threshold*, mas a supervisão ao longo do ciclo de vida da inteligência artificial.

Ademais, como adiantado, o sistema deve estar sob supervisão humana.

O Regulamento Europeu já prevê isso quanto às inteligências artificiais de risco elevado.

Esse aspecto é ainda mais relevante na identificação biométrica à distância em tempo real ante o risco concreto de falsos positivos.

Assim, a abordagem só ocorrerá depois de a correspondência ser validada por um operador humano.

Esse operador humano deve deter conhecimentos específicos sobre a tecnologia, conhecendo suas peculiaridades em termos gerais e específicas do sistema operado. Consoante adiantado, o resultado do treinamento fornecerá valiosa informação ao operador para avaliar as correspondências.

Como assinalado anteriormente, o operador humano, ao analisar o resultado obtido pelo sistema, ante seus conhecimentos, poderá identificar fatores de potencial confusão da máquina, como, por exemplo, face detectada em imagem de baixa qualidade (pela posição, luminosidade, encoberta entre outros fatores), grupos demográficos de menor precisão (mulheres negras), situação da detecção causa dúvidas na correspondência etc.

Por isso, a supervisão humana é importante fator a evitar que os sistemas de identificação biométrica à distância em tempo real operem de forma descontrolada, com potenciais a diversos falsos positivos e vieses, em prejuízo a grupos demográficos específicos, notadamente a população negra. Embora não seja uma solução por si, trata-se de relevante peça no funcionamento a fim de garantir a construção de um sistema mais equânime, justo e com medidas para mitigar a ocorrência de falsas correspondências e vieses.

Além disso, o operador humano poderá desempenhar relevante papel no monitoramento do sistema.

Isso porque ele será o primeiro indivíduo a ter contato com possíveis falsos.

Reputa-se importante, então, para fins de monitoramento, que o operador humano fique responsável pelo registro da ocorrência dos falsos, o que permitirá o melhoramento do sistema ao longo do tempo.

Nesse contexto, o operador humano deverá deter contato constante com a polícia, não apenas para informar a localização de possível alvo, mas também para saber o resultado da abordagem, catalogando as abordagens exitosas, as inexitosas (que o alvo conseguiu escapar) e os falsos.

Ao se delegar a atividade de registro ao operador humano, permite-se a construção de informações relevantes acerca do funcionamento do sistema que permitirão seu monitoramento contínuo.

Nesse contexto, deve-se haver previsão normativa sobre esse monitoramento contínuo.

Reputa-se que o monitoramento contínuo deve ensejar revisões ordinárias e extraordinárias do sistema, em que seja avaliado o seu desempenho.

As revisões ordinárias podem acontecer, por exemplo, a partir de marcos temporais (anualmente), enquanto as extraordinárias em razão de determinados acontecimentos (por exemplo, determinado número de falsos positivos, queda de precisão para determinados grupos demográficos, decisão do órgão supervisor etc.).

É importante, então, prever que o sistema seja passível dessas revisões, cuja base será a partir dos dados do monitoramento contínuo, no qual o operador humano é peça essencial.

Entende-se ser interessante aclarar esses pontos em regulação nacional, garantindo maior controle sobre o funcionamento da tecnologia.

Ainda, deve-se abordar o órgão fiscalizatório.

A existência de organismo que supervisione e fiscalize o mercado em que há sistemas de inteligência artificial de risco elevado é uma necessidade por conta das características da tecnologia anteriormente abordados.

É fundamental, outrossim, que tal organismo detenha poderes para atuar em caso de desvios, salvaguardando a população de usos indevidos de ferramentas de inteligência artificial potencialmente nociva.

Quanto à identificação biométrica à distância em tempo real, a existência de tal organismo é ainda mais relevante, dadas as peculiaridades de referida tecnologia, que não apenas envolve aspectos técnicos complexos, mas depende de uma série de decisões políticas que impactam diretamente o seu uso.

Por conta disso, inclusive, reputa-se que o organismo deve ser independente no sentido de que seus membros possam decidir as questões com autonomia, sem estar submetidos, por exemplo, à hierarquia da Administração Pública ou submissos aos governos, de modo a garantir que a supervisão da tecnologia aconteça com base em interesses que melhor reflitam aspectos técnicos e interesses sociais, sem pender, desfavoravelmente, para incremento da vigilância.

Esse organismo independente se mostra fundamental exatamente para contrabalancear os riscos de vigilância massiva que a tecnologia carrega consigo.

Vistos em tópicos anteriores, há projetos legislativos prevendo tal atribuição ao CNJ ou à ANPD.

Independente de qual órgão seja, entende-se fundamental garantir, especificamente quanto à identificação biométrica à distância em tempo real, que o organismo, além de independente em relação ao governo, detenha tanto conhecimentos técnicos direcionados à tecnologia, quanto participação da sociedade civil.

A necessidade de conhecimentos técnicos específicos decorre da particularidade da tecnologia, cuja aplicação adequada depende da observância de diversos critérios técnicos rigorosos.

Há diversos aspectos ligados a conhecimentos técnicos próprios de mencionada tecnologia, como a coleta de imagens de qualidade e com representatividade para formação do banco de dados, realização de treinamentos prévios com coleta da precisão do reconhecimento geral e específica para grupos demográficos, medidas para redução de vieses contra grupos demográficos, fixação do grau de similaridade para estabelecer uma correspondência positiva, determinação dos locais das câmeras, qualidade das câmeras para coleta das imagens, monitoramento contínuo do sistema e revisão periódica etc.

Nesse contexto, as especificidades técnicas, que impactam diretamente o funcionamento da tecnologia e seus potenciais riscos a direitos fundamentais e humanos, podem ser regulados pelo organismo de supervisão independente, que dará diretrizes a serem observadas, bem como fiscalizará esses aspectos técnicos ao longo do ciclo de vida dos sistemas de inteligência artificial voltados para tal finalidade.

Inclusive, como visto anteriormente sobre a necessidade de transparência, existem aspectos técnicos que são ininteligíveis ao público em geral e dependem de conhecimentos específicos para supervisão.

Esse organismo exerceria esse papel de fiscalização do dever de transparência quanto aos aspectos técnicos mais intricados da tecnologia, representando a coletividade no controle dos sistemas.

Embora a população, em geral, não consiga compreender detalhes mais complexos do funcionamento do sistema, a existência de organismo independente com tal função vem para garantir que o funcionamento está sendo adequado e que as premissas de transparência estão sendo cumpridas, pois os desenvolvedores e implantadores ostentarão o dever de informação a tal organismo.

Sob esse prisma, referido organismo poderá ser o local para que os indivíduos afetados pela tecnologia possam exercer seu direito de recurso, questionando aspectos do funcionamento do sistema.

Exatamente pela presença de conhecimentos técnicos específicos e por estar informado dos detalhes do sistema em razão do dever de transparência dos desenvolvedores e implantadores, o organismo independente poderá decidir a questão de forma justa.

Ademais, nos termos já estudados, a tecnologia não é neutra e revolve, em verdade, uma série de decisões políticas, o que é ainda mais verdadeiro para a identificação biométrica à distância em tempo real.

Dessa forma, além dos conhecimentos técnicos específicos, o organismo ficará a cargo de decisões políticas sobre o funcionamento da tecnologia, como definição dos níveis de precisão do equipamento para poder ser utilizado, medidas para evitar vieses, *tradeoff* relativo ao grau de similaridade etc.

Aliás, exatamente pelo potencial de afetação desigual da tecnologia a depender do grupo demográfico, desponta a necessidade de decisões política não apenas na implantação do sistema, mas ao longo de seu ciclo de vida. O exercício desse papel, sobretudo no monitoramento, fica mais bem adequado com organismo capaz de supervisionar a tecnologia de forma contínua, com conhecimentos técnicos e também com representatividade política.

Isso é um detalhe muito relevante acerca da tecnologia em voga, porque não apenas na decisão de seu uso haverá juízo político, mas, ao longo do seu funcionamento, que deverá ser

continuamente monitorado, também despontarão questões cujo encaminhamento envolverá inevitavelmente juízos políticos.

Uma vez implantada a tecnologia, deve-se garantir que sua utilização não está acarretando vieses e estigmatizando determinados grupos, de modo a acentuar desigualdades sociais e prejudicar certas populações demográficas, o que implica, necessariamente, a aferição de juízos de valor de índole política sobre a tecnologia.

Por essa razão, entende-se que, além dos conhecimentos técnicos, o organismo de supervisão deve contar com participação de membros da sociedade civil, no intuito de garantir que a tecnologia não desdobre para vigilância em massa, arbítrios ou mesmo discriminação contra determinados grupos demográficos.

Essa previsão reforça o aspecto democrático do organismo supervisor, fortalecendo, assim, a legitimidade do uso da tecnologia tão controversa.

A hipótese de participação da sociedade civil no organismo de supervisão se cuida de importante elemento a aumentar o grau democrático e de legitimidade da tecnologia, estabelecendo que o exercício de juízos políticos não se encerra na permissão legislativa para uso da tecnologia, mas segue durante o ciclo de vida de referida inteligência artificial.

A pertinência de tal participação é reforçada pelo grau de incipiência da tecnologia, a recomendar que, nesse momento, utilizem-se medidas de maior cautela e com maior participação da coletividade; do contrário, ao se permitir o uso sem estritas balizas e participação democrática, pode haver efeito *backlash* a conduzir ao banimento da tecnologia, como visto em determinadas localidades.

Em suma, reputa-se essencial a fixação de um organismo independente de supervisão que valide o sistema previamente ao uso. Inclusive, em tal organismo, poderão ser adotadas as decisões políticas acerca do uso do sistema (como o *trade-off* adequado do *threshold)*, bem como o controle e monitoramento da tecnologia, ao qual poderão ser comunicadas as falsas correspondências do sistema e outras falhas, de modo a se encarregar do processo de revisão periódica e realização dos ajustes necessários. Em tal organismo, inclusive, para prestigiar o caráter democrático, revela-se pertinente a inclusão de membros da sociedade civil com conhecimentos sobre a área, fortalecendo a pluralidade do órgão e evitando eventuais usos abusivos da tecnologia.

Por fim, um último aspecto que ostenta relevância diz respeito à avaliação de risco.

Embora não constante na proposta inicial da Comissão Europeia, a avaliação de risco a direitos fundamentais dos sistemas de risco elevado foi incluída na redação final e atualmente consta no Regulamento Europeu.

Apesar de se tratar de ponto extremamente positivo, foi apontado, em tópico anterior, que referida avaliação peca em dois sentidos: não é específica para a identificação biométrica à distância em tempo real e não precisa ser validada antes do uso da tecnologia.

Sobre o primeiro ponto, destaca-se que, ao longo do estudado no presente trabalho, a tecnologia em voga apresenta diversos aspectos próprios, como níveis de precisão, *tradeoff*, localização de câmeras, coleta e formação do banco de dados etc., que revolvem questões próprias a serem balanceadas.

Avaliações genéricas de risco não conseguiriam, a nosso ver, captar a complexidade do tema, de modo que se reputa necessário que a avaliação do sistema dedicado a tal finalidade deva responder as questões específicas que aqui foram levantadas.

Do contrário, detalhes relevantes podem ser deixados de lado, e a avaliação se mostrar inócua para realmente validar o sistema.

Nesse prisma, ao organismo de supervisão, até porque com conhecimentos específicos da tecnologia, cabe fixar os quesitos a serem abordados na avaliação de risco, tornando-a própria para a tecnologia em voga.

Um segundo ponto diz respeito ao papel da avaliação de risco.

Reputa-se que ela seja previamente validada pelo organismo de supervisão para que o sistema possa ser utilizado.

Assim, não bastará a realização da avaliação pelo desenvolvedor e implantador; referida avaliação deve ser submetida previamente ao crivo do organismo de supervisão que deverá validá-la para que o uso aconteça.

Em tal toada, o organismo de supervisão já exerce o controle da tecnologia antes de seu uso, de modo a garantir a colocação no mercado do sistema de forma mais segura e sem risco de acentuadas violações a direitos fundamentais e humanos.

Embora possa se questionar a praticidade da validação prévia da avaliação de risco para todos os sistemas de risco elevado (o que pode ter levado o Regulamento Europeu a prever apenas a necessidade de sua realização), considera-se que, para a identificação biométrica à distância em tempo real, essa validação não é apenas fundamental (dados os acentuados riscos

do sistema, como visto), mas factível, na medida que, pelo alto investimento da tecnologia, não se imagina que haverá diversos sistemas dedicados à finalidade.

Então, especificamente para a identificação biométrica à distância em tempo real, a validação da avaliação de risco prévia ao uso por organismo independente de supervisão é fator essencial para salvaguarda de direitos fundamentais e humanos.

Entende-se que, tomando-se o Regulamento Europeu de Inteligência Artificial e adotando as precauções aqui assinaladas, é possível a fixação de marco normativo no Brasil sobre o uso da identificação biométrica à distância em tempo real em consonância com a proteção de direitos fundamentais e humanos, resguardando os indivíduos e a coletividade de aspectos nocivos da tecnologia, cujo uso apresenta potenciais para cumprimento dos deveres estatais na consecução da segurança pública.

6. CONSIDERAÇÕES FINAIS

O presente trabalho dedicou-se a avaliar a compatibilidade das previsões de uso de reconhecimento facial na segurança pública pelo Regulamento Europeu da Inteligência Artificial com a proteção de Direitos Humanos e sua eventual compatibilidade com o ordenamento jurídico brasileiro, de modo a servir como fonte de inspiração legislativa.

No segundo capítulo da obra, conceituou-se a segurança pública, caracterizando-a como a atividade estatal voltada à prevenção e à repressão de delitos. Em termos jurídicos, a segurança pública revela direito fundamental e humano multigeracional, em que emergem obrigações processuais penais positivas do Estado em agir face os potenciais delitivos na tutela da vítima e da sociedade.

Sob esse aspecto, enquanto, em primeira geração, o direito à segurança pública reflete o direito individual de ação estatal após a ocorrência do risco, em segunda geração trata-se do direito social de montagem da política pública de segurança que será exigível individualmente por quem porventura ser vítima de crime, ao passo que, em terceira geração, o direito à segurança pública se relaciona com medidas de índole coletiva e difusa, que superam as perspectivas individuais e reclamam ações efetivas e estruturantes para a sociedade como um todo.

Logo, supera-se a perspectiva do direito à segurança pública como mera vedação a arbitrariedades estatais, o que o limita tão somente a uma faceta de primeira geração de índole negativa.

Presente que, do direito fundamental e humano da segurança pública, emergem obrigações de agir do Estado, buscou-se avaliar como as tecnologias de reconhecimento facial poderiam auxiliar no cumprimento de tal mister.

Inicialmente, sumarizou-se que as tecnologias de reconhecimento facial, atualmente, impulsionadas pela inteligência artificial, passaram a ser desenvolvidas para uma série de finalidades e com diversos propósitos, de modo que o tema não é inequívoco, mas depende de uma precisa definição do objeto para avaliar os impactos da tecnologia respectiva nos direitos dos indivíduos.

Em aprofundamento sobre o tema, ressaltou-se que as tecnologias de reconhecimento facial englobam um conjunto de tecnologias distintas insertas no campo da identificação

biométrica, destinadas a identificar/categorizar o indivíduo por meio de suas características faciais. Por meio de processos automatizados e com base em modelos estatísticos, cuja coleta de dados acontece de forma não intrusiva, gera-se uma identidade facial (*faceprint*) com os traços distintivos do rosto do indivíduo a ser comparada com as imagens (padrões) existentes no banco de dados e cuja correspondência – positiva ou negativa – será dada a partir de um escore de similaridade, de modo que o sistema não oferece resultados definitivos, mas apenas probabilidades.

Dentro desse conceito, existem diversas tecnologias aplicadas para usos distintos, como verificação da identidade de uma pessoa singular, identificação de uma pessoa em meio à multidão ou reconhecimento e categorização de emoções, bem como direcionadas para finalidades diversas (concessão de acesso a locais, diagnóstico de doenças, segurança pública etc.). Por isso, a análise de impacto deve acontecer de forma individualizada a partir do uso e da finalidade do sistema

No presente trabalho, estuda-se a identificação do indivíduo em meio à multidão para fins de segurança pública.

Cuida-se de reconhecimento facial remoto e em tempo real, exatamente aquele tipo de atividade que desperta grande preocupação da doutrina pelo seu caráter de possível vigilância expansiva e insidiosa, sem o conhecimento dos indivíduos e com possibilidade de alto impacto em direitos e liberdades individuais.

Para fins de precisão conceitual, adotou-se o termo técnico de referido sistema como "sistema de identificação biométrica à distância em tempo real".

Uma vez delimitado o objeto do presente trabalho, aprofundou-se nas questões relativas à inteligência artificial, uma vez que se trata do embasamento tecnológico por trás de mencionado sistema.

Para fins de conceito do presente trabalho, após se expor as controvérsias sobre o tema, resumiu-se que o sistema de inteligência artificial se caracteriza pela capacidade de inferência baseada em máquinas, destinado à solução autônoma de problemas diante de objetivos fixados pelo operador e a partir de uma base de conhecimento estabelecida, com potencial para aprender em função dos resultados gerados, aprimorando continuamente o seu desempenho na finalidade pretendida.

Esses sistemas, contudo, carregam consigo perigos inerentes, pois são complexos, uma vez que a capacidade de processamento é muito superior à capacidade humana, e opacos, na

medida em que não há como rastrear precisamente os motivos do resultado obtido pela máquina, exatamente por se tratar de inferência e não do resultado da observância de um código estrito.

Ademais, os sistemas de inteligência artificial exibem comportamento autônomo e imprevisível, que vai, ao longo do tempo, alterando-se; consequentemente, exatamente por esse aspecto de aprendizagem, o sistema depende de dados de qualidade para funcionar adequadamente

Nesse contexto, defluem os riscos de tais sistemas, uma vez que a complexidade, opacidade e autonomia geram comportamentos imprevisíveis, com potencial resultado não esperado, além do fato de que a dependência de dados de qualidade para operar de forma adequada impõe a necessidade de controle e treinamento dos sistemas.

Os riscos, por sua vez, refletem decisões políticas de como enfrentar perigos e inseguranças contemporâneos. Contextualizando ao caso, o fato de os sistemas de inteligência artificial apresentarem perigos e incertezas não seria suficiente para barrar o seu uso, diante dos potenciais inovadores que trazem, de modo que a solução ocorre pela via política mediante administração do risco.

Quanto à segurança pública, os sistemas de inteligência artificial trazem arcabouço técnico a auxiliar o Estado no cumprimento das obrigações processuais penais positivas, sem, todavia, deixar de ensejar riscos inerentes, até mais acentuados, em razão da importância dos bens jurídicos tutelados pela esfera penal e seu caráter de *ultima ratio*.

Fixadas, então, as particularidades da inteligência artificial, adentrou-se propriamente no objeto do presente estudo, qual seja, a identificação biométrica à distância em tempo real para fins de segurança pública.

Estabeleceu-se que a implementação de sistemas de identificação biométrica à distância em tempo real segue os passos do ciclo de vida da inteligência artificial, pois dependentes de tal tecnologia.

Desse modo, os sistemas devem ser objeto de desenho, preparação de dados, modelamento e validação, operação e monitoramento, e revisão, de forma contínua, para garantir o desempenho adequado de suas funções. A dependência de dados é uma característica importante e que desperta questões cruciais, uma vez que os dados biométricos são sensíveis e passíveis de proteção especial, necessitando-se, portanto, de maiores cuidados no momento da coleta.

O funcionamento da inteligência artificial, por sua vez, se funda em abordagens holísticas (por vezes combinadas com método de análise de características faciais) em processo de aprendizagem pela máquina, notadamente por meio de redes neurais profundas, o que reforça a dependência de dados e de adequado treinamento do algoritmo.

Além disso, é importante que o resultado do sistema passe por supervisão humana, não gerando ações automáticas. Um último ponto reflete a questão relativa às localizações das câmeras, que, se focarem apenas em áreas marginalizadas, podem servir para incrementar desigualdades, com risco de maiores vieses em abordagens.

A implementação do sistema de identificação biométrica à distância em tempo real passa por esses estágios, que, como se percebe, revelam a complexidade do tema, na medida em que há diversas etapas interligadas e que a falha em uma delas é capaz de prejudicar o desempenho do sistema como um todo.

Em seguida, adentrou-se nas circunstâncias específicas que são relevantes para definir a possibilidade e a extensão do uso dos sistemas de identificação biométrica à distância em tempo real.

Sinalizando-se a inexistência de neutralidade e o caráter político da tecnologia, foram analisados, sob o prisma técnico do sistema: os seguintes aspectos: *trade-off threshold* (falsos positivos/falsos negativos), qualidade de dados (banco de dados), vieses (erro algorítmico e localização das câmeras) e a necessidade de supervisão humana.

Assentou-se que, ao operar com probabilidades, o sistema definirá, a partir de um escore de similaridade, a correspondência de uma face ao constante no banco de dados, de modo que quanto maior for a baliza (*threshold*), maior será a possibilidade de falsos negativos, enquanto, ao se diminuir a baliza, aumentam-se os falsos positivos. Há, então, inequívoco *trade-off*, a denotar os efeitos políticos e jurídicos da fixação da baliza sobre direitos fundamentais e humanos afetados pela incidência dos erros da máquina cotejados com o propósito do sistema e sua eficiência em cumprir tal propósito.

Destacou-se, ainda, que, por depender de dados de qualidade, a confecção do sistema depende da construção de banco de dados com imagens de qualidade, representativas, com padrões específicos para diferentes grupos demográficos, e cuja coleta respeite direitos individuais e da coletividade.

Apontou-se, em seguida, a existência de vieses do sistema em face de determinados grupos demográficos decorrentes da falta de precisão da tecnologia, em especial para negros e

mulheres, concluindo-se pela necessidade de representatividade social nos dados utilizados e não utilização exacerbada da tecnologia em áreas de concentração de minorias.

Por fim, enfatizou-se a supervisão humana com importante fator a evitar que os sistemas de identificação biométrica à distância em tempo real operem de forma descontrolada, com potenciais a diversos falsos positivos e vieses, em prejuízo a grupos demográficos específicos, notadamente a população negra.

Sob o prisma jurídico, analisou-se as intersecções da tecnologia com direitos humanos pelos seguintes aspectos: autonomia/privacidade (qualidade de dados e consenso), direitos à liberdade de expressão e à reunião (*chilling effect*), discriminação, princípio da presunção de inocência, princípios da transparência e da explicabilidade, grupos etários (crianças e idosos).

Apontou-se que a utilização da mencionada tecnologia implica intromissão no direito à privacidade e no direito à proteção de dados sensíveis, cuja ocorrência será justificada a partir das finalidades adotadas pelo sistema (investigar fatos graves, em que a afetação aos referidos direitos fundamentais e humanos se revele proporcional, no intuito de cumprir também o direito fundamental e humano à segurança pública).

Sinalizou-se, outrossim, que, ao construir sistema de identificação biométrica à distância em tempo real, deve-se ter presente seu efeito deletério para exercício de liberdades individuais e coletivas decorrentes do impacto na percepção individual acerca da ocupação do espaço público. Em tal mister, a fixação de finalidades específicas para atuação do sistema, que não implique monitoramento de pessoas engajadas em atos de liberdade de expressão e direito de reunião, é essencial para que a população não perca senso comunitário do espaço público, evitando, então, risco de arrefecimento no exercício das liberdades democráticas.

Quanto ao potencial discriminatório do sistema, ressaltou-se que controles apropriados, como revisões múltiplas, operadores treinados e processos de garantia de qualidade, devem ser garantidos antes de se colocar o sistema em funcionamento, o que é fundamental para confiança do público e utilização do sistema de maneira justa e justificada. Logo, durante as diversas etapas de construção e implementação do sistema, devem ser tomadas medidas para evitar vieses em face de determinados grupos a causar discriminações juridicamente vedadas.

Esclareceu-se que o sistema, por si, ao ficar sob supervisão humana e não gerar conclusões automáticas, não viola o princípio da presunção da inocência, fornecendo justa causa à abordagem policial. Enfatizou-se que não apenas a construção do sistema e o monitoramento do seu ciclo de vida devem ocorrer de forma criteriosa a fornecer resultados

robustos, como as próprias correspondências positivas devem ser validadas pelo operador humano antes de qualquer ação policial.

Asseverou-se que sistema de identificação biométrica à distância em tempo real deve ostentar níveis de transparência e explicabilidade para permitir que os indivíduos afetados compreendam seu funcionamento e a forma de obtenção do resultado; do contrário, os resultados do sistema tornar-se-ão obscuros e passíveis de questionamento perante os tribunais.

A transparência e a explicabilidade de forma mais profunda não serão exercidas pelo cidadão em si, que careceria de conhecimentos técnicos para compreensão aprofundada sobre o funcionamento da máquina, mas sim por entidades que exerçam fiscalização contínua do sistema, que estão aptas a exercer escrutínio mais denso sobre as peculiaridades da inteligência artificial, com conhecimentos profundos sobre a matéria.

Por isso, é fundamental que se constituam organismos idôneos e com representatividade para exercício dessa função, na medida em que funcionarão como representantes da sociedade para garantir o funcionamento adequado do sistema de identificação biométrica à distância em tempo real.

Relativamente aos grupos etários, destacou-se menor precisão do sistema para face de crianças e idosos, o que, por outro lado, não justificaria a vedação do uso da tecnologia, mas imporia a necessidade de cuidados especiais quanto a tais grupos.

Ao ponderar riscos e potenciais benefícios do sistema, concluiu-se que não se trata de vedar peremptoriamente o uso da identificação biométrica à distância em tempo real, mas adequá-la a um cenário que, a um só tempo, se busque maior eficácia na promoção da segurança pública sem implicar, por outro lado, em violações descabidas de direitos fundamentais e humanos.

Por esse prisma, a edição de regulação sobre o tema, ponderando as questões inerentes, será reservada aos casos estritamente necessários, direcionados a crimes graves e com alvo específico, observando, ainda, a necessidade de proteção de grupos vulneráveis. Deve-se demonstrar que a finalidade de processamento de dados sensíveis não pode ser alcançada por meios menos intrusivos em direitos fundamentais, com parâmetros para captação das imagens e período de retenção, direito à informação, transparência e explicabilidade, mecanismos para garantir a precisão do sistema, no intuito de evitar falsos positivos, e supervisão humana.

Estabelecida possível a regulação da matéria mediante a fixação de usos restritos, abordou-se o Regulamento Europeu da Inteligência Artificial, primeiramente contextualizando o diploma e após adentrando nas previsões específicas sobre o objeto de estudo.

Estabeleceu-se, em regra, a vedação ao uso da identificação biométrica à distância em tempo real, salvo para os seguintes fins: "1) busca seletiva de vítimas específicas de rapto, tráfico de seres humanos ou exploração sexual de seres humanos, bem como a busca por pessoas desaparecidas; 2) prevenção de uma ameaça específica, substancial e iminente à vida ou à segurança física de pessoas singulares ou de uma ameaça real e atual ou real e previsível de um ataque terrorista; e 3) a localização ou identificação de uma pessoa suspeita de ter cometido uma infração penal, para efeitos da realização de uma investigação criminal, ou instauração de ação penal ou execução de uma sanção penal por alguma das infrações referidas no anexo II e puníveis no Estado-Membro em causa com pena ou medida de segurança privativa de liberdade de duração máxima não inferior a quatro anos".

Em tais casos, uso da tecnologia deve ter alvo específico, isto é, pessoas individualizadas e pré-determinadas, fundado em circunstâncias decorrentes de comportamento real e não baseado em julgamentos preditivos ou com base em meras características pessoais.

O mero preenchimento de alguma das hipóteses de uso da tecnologia e a prévia identificação da pessoa visada não é suficiente para validar a utilização da tecnologia, uma vez que se depende de determinadas balizas para deferimento.

O item 2 da alínea *h* do artigo 5º do Regulamento aponta que, para uso da tecnologia, devem ser considerados os seguintes elementos: "1) A natureza da situação que origina a possível utilização, em especial a gravidade, a probabilidade e a magnitude dos danos causados na ausência da utilização do sistema; e 2) As consequências da utilização do sistema para os direitos e as liberdades de todas as pessoas afetadas, em especial a gravidade, a probabilidade e a magnitude dessas consequências".

O dispositivo revela verdadeira ponderação para autorizar o uso da tecnologia, de modo que, para cada caso, deve haver essa ponderação individualizada.

Além disso, o sistema de identificação biométrica à distância em tempo real deve, nos termos do último parágrafo do item 2 da alínea *h* do artigo 5º, ser submetido à prévia avaliação de impacto sobre os direitos fundamentais para ser utilizado, com registro na base de dados da União Europeia.

Nessa senda, enquanto para cada caso individualizado haverá ponderação particular dos benefícios e prejuízos, o sistema como um todo deve passar previamente por avaliação de impacto sobre direitos fundamentais, considerando os usos pretendidos, isto é, as três hipóteses excepcionais de uso mencionadas.

Por sua vez, os Estados-Membros da União Europeia, antes de iniciar o uso, devem criar legislação específica sobre a tecnologia e o procedimento para autorizar o seu uso e, em tal contexto, podem autorizar total ou parcialmente as hipóteses excepcionais de uso da identificação biométrica à distância em tempo real, inclusive indicando quais delitos do anexo III justificam o uso da tecnologia.

Quanto ao procedimento para uso da tecnologia, o cumprimento das balizas assinaladas e a verificação da pertinência do uso da tecnologia para as hipóteses excepcionais, com base em elementos probatórios mínimos acerca da presença de causa justificadora, passa por autorização judicial prévia, de modo a permitir o uso ao estritamente necessário em termos temporais, geográficos e pessoais.

Assim, cada uso individualizado deverá ser autorizado por autoridade judiciária (ou a ela equivalente) e será comunicada à autoridade de fiscalização do mercado pertinente e à autoridade nacional de proteção de dados, contendo informações acerca da utilização, sendo que as autoridades nacionais devem apresentar relatórios anuais à Comissão Europeia sobre o uso da tecnologia, com o número de decisões tomadas pelas autoridades judiciais competentes sobre a utilização.

Ademais, uma vez em uso, o sistema de identificação biométrica à distância em tempo real deve observar os demais requisitos dos sistemas de risco elevado. Isso porque, se o sistema de inteligência artificial usado na segurança pública não for de risco proibido (isto é, não esteja listado em alguma das hipóteses do artigo 5º do Regulamento), ele será, em regra, de risco elevado, exatamente como ocorre com a identificação biométrica à distância nas hipóteses permitidas, impondo, consequentemente, o cumprimento dos diversos deveres para os implantadores de sistemas de risco elevado.

Em seguida, analisou-se a compatibilidade do Regulamento com a proteção de direitos humanos.

As críticas ao Regulamento podem ser resumidas nos seguintes pontos: 1) falta de estudos sobre a efetividade da tecnologia; 2) abertura de margens discricionárias para aplicação pelos Estados, notadamente ante a zona cinzenta do conceito de segurança nacional; 3) falta de

regras claras e precisas a potencializar confusões e violações a direitos fundamentais; 4) rol de hipóteses de exceção amplamente largo, sem situações de urgência; 5) desconsideração que, uma vez fixada a infraestrutura da tecnologia, ela tenderá a ser reproduzida, gerando *chilling effect*; e 6) ausência de validação da avaliação de impacto em direitos fundamentais por organismo de supervisão independente.

Em análise às críticas, verificou-se problemática a exclusão da segurança nacional da disciplina do Regulamento, bem como o fato de que não foram previstas obrigações aos desenvolvedores e implantadores específicas sobre a identificação biométrica à distância em tempo real, cujo ciclo de vida da inteligência artificial demanda cuidados particularizados, como evitar vieses, preocupação com grupos demográficos e etários, ponderação do *tradeoff* do *threshold*, necessidade de construção de base de dados de qualidade com observância de peculiaridades da segurança pública e de representatividade de diferentes grupos demográficos etc.

Além disso, a mera comunicação da avaliação de impacto em direitos fundamentais não parece ser suficiente a mitigar os riscos da tecnologia, que deveria ser validada por organismo de supervisão independente, inclusive para verificar se o desenho, coleta de dados e treinamento do sistema de inteligência artificial foi realizado de acordo com as diretrizes de direitos humanos e fundamentais incidentes na espécie.

Apesar das críticas, algumas delas pertinentes, o Regulamento se mostra, em grande medida, adequado e pertinente para finalidade que se propõe, sem prejuízo de que haja eventuais espaços para melhorias e maior segurança jurídica e proteção de direitos fundamentais e humanos. Assim, entendeu-se que o Regulamento, apesar de eventuais pontos de melhoria, se mostra, em linhas gerais, atento aos direitos humanos e fundamentais em voga, sem prejuízo de potenciais aperfeiçoamentos ao longo de sua implementação.

Os pontos falhos do Regulamento, notadamente por se tratar de legislação genérica e não específica da identificação biométrica à distância em tempo real, podem ser abordados em solo nacional por meio de lei específica para a temática.

Logo, referidos pontos falhos, embora dignos de nota, não justificam considerar o Regulamento como contrário aos direitos fundamentais e humanos, pois o diploma, de fato, revelou preocupação com aspectos particularizados do uso da identificação biométrica à distância em tempo real e sua interferência em direitos humanos e fundamentais; apenas alguns deveres específicos inerentes à gestão do ciclo de vida de tal inteligência artificial, dadas as

suas peculiaridades, demandariam previsões normatizadas particularizadas, o que não acabou ocorrendo, sem prejuízo de que, ao longo da implementação do Regulamento, isso seja corrigido, seja por meio da alteração do Diploma, normativas das legislações domésticas dos países ou mesmo, eventualmente, por atos delegados da Comissão Europeia a partir do paradigma do Novo Quadro Legislativo.

Assentada, então, em essência, a observância dos direitos humanos e fundamentais pelo Regulamento, sem prejuízo dos pontos de melhoria assinalados, analisou-se como referida legislação pode influenciar o debate no cenário nacional, considerando, inclusive, os pontos falhos e as diferentes particularidades entre a fixação de uma legislação transnacional (caso do Regulamento) e a elaboração de legislação interna (caso do Brasil).

No Brasil, verificou-se que já há usos da tecnologia, sem haver, por outro lado, qualquer disciplina normativa específica, o que tem gerado debates no cenário nacional.

Aqui, a solução legislativa também caminha para a elaboração de um diploma normativo genérico da inteligência artificial, que replica as diretrizes do Regulamento Europeu.

Nesse contexto, embora o referido Diploma se trate de relevante fonte normativa, entende-se que a sua previsão genérica em determinados pontos, sem abordar questões específicas da identificação biométrica à distância em tempo real e de seus riscos particulares, acabou por deixar brechas na implementação do sistema que podem gerar violações a direitos fundamentais.

Portanto, a edição de normativa do Brasil deve se atentar a tais peculiaridades, além da própria realidade nacional e do fato de o Regulamento ser diploma transnacional. É fundamental que a aplicação da tecnologia ocorra em contexto de adequado controle das ferramentas de política criminal, com usos rigorosos e voltados para maior efetividade do sistema, em esforços de *compliance* criminal.

Em tal toada, mostra-se adequada a elaboração de disciplina normativa específica para a identificação biométrica à distância em tempo real (ainda que, eventualmente, constante em diploma mais genérico), com consideração, sob o ponto de vista técnico, da inexistência de neutralidade da tecnologia, do *trade-off threshold* (falsos positivos/falsos negativos), da qualidade de dados (banco de dados), dos vieses (erro algorítmico e localização das câmeras), da necessidade de supervisão humana, e, sob o ponto de vista jurídico, das seguintes interferências: autonomia/privacidade (qualidade de dados e consenso), direitos à liberdade de

expressão e à reunião (*chilling effect*), discriminação, princípio da presunção de inocência, princípios da transparência e da explicabilidade, grupos etários (crianças e idosos).

Sugere-se a inexistência de exclusão de questões de segurança nacional, bem como a presença de requisitos específicos para desenho, coleta de dados, treinamento, validação, monitoramento e revisão da tecnologia, dadas as peculiaridades da identificação biométrica à distância em tempo real. Além das finalidades de uso restritas e de procedimento rígido individualizado para uso da tecnologia mediante autorização judicial (pontos positivos do Regulamento que podem ser replicados), devem ser estipuladas regras específicas pertinentes ao controle de ciclo de vida da tecnologia em si, que, por ser particular e com alto grau de impacto, requer cuidados especiais.

Notadamente, devem haver medidas para: 1) estipulação do *trade-off* adequado do *threshold* (falsos positivos/falsos negativos), o que impõe uma decisão política acerca de eventuais equívocos do sistema (se para positivos ou se para negativos); 2) construção de banco de dados com imagens de qualidade, representativas, com padrões específicos para diferentes grupos demográficos, e cuja coleta respeite direitos individuais e da coletividade; 3) restrições específicas para evitar vieses, demandando-se representatividade social nos dados utilizados e não utilização exacerbada da tecnologia em áreas de concentração de minorias; 4) disposições específicas de treinamento e da supervisão humana na identificação biométrica à distância em tempo real, com conhecimentos especializados sobre os potenciais de falsos positivos e vieses, evitando-se em prejuízo a grupos demográficos específicos, notadamente a população negra.

Além disso, reputa-se essencial a fixação de um organismo independente de supervisão que valide o sistema previamente ao uso. Inclusive, em tal organismo, poderão ser adotadas as decisões políticas acerca do uso do sistema (como o *trade-off* adequado do *threshold)*, bem como o controle e monitoramento do uso da tecnologia, ao qual poderão ser comunicadas as falsas correspondências dos sistemas e outras falhas, de modo a se encarregar do processo de revisão periódica e realização dos ajustes necessários. Em tal organismo, inclusive, para prestigiar o caráter democrático, revela-se pertinente a inclusão de membros da sociedade civil com conhecimentos sobre a área, fortalecendo, portanto, a pluralidade do órgão e evitando eventuais usos abusivos da tecnologia.

Com adoção de tais precauções, entende-se que haverá bases jurídicas suficientes a justificar a utilização da identificação biométrica à distância em tempo real em prol da segurança pública sem resultar em violações aos seguintes direitos: autonomia/privacidade (qualidade de dados e consenso), direitos à liberdade de expressão e à reunião (*chilling effect*),

discriminação, princípio da presunção de inocência, princípios da transparência e da explicabilidade, grupos etários (crianças e idosos).

Como limitações ao presente estudo, pode-se ressaltar que o trabalho não exauriu a abordagem de todos os pontos do Regulamento, especialmente sobre os requisitos dos sistemas de risco elevado que incidem genericamente sobre a identificação biométrica à distância em tempo real. Também houve uma contingência temporal no estudo, decorrente da recente aprovação do Regulamento, que ainda carece de maior aprofundamento da doutrina, bem como de situações práticas de aplicação e jurisprudência sobre sua normativa. A novidade do tema causou, então, maiores dificuldades no exame, que certamente evoluirá no futuro. Além disso, a análise de legislação de índole transnacional de comunidade da qual o Brasil não faz parte impôs desafios no tocante ao conhecimento integral da legislação pertinente e de todas as suas peculiaridades. Outrossim, impende destacar que opções normativas de regulação da matéria adotada por outros países, como China, Rússia e Estados Unidos da América não foram exploradas, embora, em termos práticos, essas opções possam ter impacto em solo nacional, dada a tendência de unificação das normas penais por força do processo de globalização e da crescente existência da criminalidade transnacional.

Como pontos para futuras pesquisas, indica-se aprofundamento sobre situações práticas de utilização da tecnologia com base no Regulamento e os resultados delas decorrentes, com as controvérsias respectivas. Também se aponta como relevante o estudo das opções de regulação adotadas por outros países (China, Rússia e Estados Unidos da América), cotejando-as com as soluções do Regulamento Europeu, a fim de avaliar a melhor forma de regulamentação da matéria, até em conta dos efeitos da globalização e dos crimes transnacionais.

REFERÊNCIAS

ACYPRESTE, R.; PARANÁ, E. Artificial Intelligence and employment: a systematic review. *In*: **Brazilian Journal of Political Economy**, v. 42, n. 4, p. 1014–1032, dez. 2022.

AKBARI, A. Facial Recognition Technologies 101: Technical Insights. *In*: **The Cambridge Handbook of Facial Recognition in the Modern State**. Editado por RITA MATULIONYTE e MONIKA ZALNIERIUTE. Cambridge University Press, 2024.

ALEXY, R. **Teoria de los derechos fundamentales**. Madrid: Centro de estúdios constitucionales, 1997.

ALZOU'BI, S. ALSHIBLY, H. AL-MA'AITAH. Artificial Intelligence in Law Enforcement, a Review. *In***: International Journal of Advanced Information Techonology (IJAIT)**, v. 4, n. 4, ago., 2014.

AVILA, T. A. P. A atuação do Ministério Público na concretização do direito fundamental à segurança pública. *In*: **Revista do CNMP**, n. 4, 2014.

AZEVEDO. R. G.; BASSO. M. Segurança Pública e Direitos Fundamentais. *In*: **Direito & Justiça**, Porto Alegre, v. 34, n. 2, p. 21-32, jul.-dez. 2008.

AZEVEDO, C. P. G.; LIMA, E. M. B.; SILVA, F. R.; RODRIGUES, G. R.; DUTRA, L. C. M.; SANTARÉM, P. R. S.; RODRIGUES, V. B. V. R. **Nota técnica: análise comparativa entre o anteprojeto de LGPD penal e o PL 1515/2022**. Instituto de Referência em Internet e Sociedade (IRIS) e Laboratório de Políticas Públicas e Internet (LAPIN), nov. 2022. Disponível em: <bit.ly/3U0OuU0>. Acesso em: 06 out. 2024.

BARRETO, A. C. R.; BORGES, K. E. Comentário ao artigo III. *In*: BALERA, W. (Organizador). **Comentários à Declaração Universal dos Direitos Humanos e Jurisprudência**. 3ª ed. São Paulo: KDP Amazon, 2018.

BARRETO FILHO, H. **Polícia usa reconhecimento facial para prender foragidos no meio da folia**. UOL, São Paulo, 10 fev. 2024. Disponível em: <https://noticias.uol.com.br/cotidiano/ultimas-noticias/2024/02/10/reconhecimento-facial-prisoes-foragidos-brasil.htm?cmpid=copiaecola>. Acesso em: 28 abr. de 2024.

BECHARA, F. R.; SMANIO, G. P.; GIRARDI, K. B. Cooperação jurídica internacional na Operação "Lava Jato": análise crítica a partir da diversidade entre os sistemas jurídicos nacionais. *In*: **Revista Brasileira de Direito Processual Penal**, v. 5, n. 2, mai.-ago., 2019, pp. 703-736.

BECK, U. **Risk society. Towards a new modernity**. Traduzido por Mark Ritter. Londres: Sage Publications, 1992.

BERK, R. A. Facial Recognition Technologies 101 Technical Insightst. *In*: **Annual Review of Criminology**. 2021, pp. 209-237. Disponível em: https://www.annualreviews.org/content/journals/10.1146/annurev-criminol-051520-012342. Acesso em: 28 abr. 2024.

BRADFORD, A. **The Brussels effect: how the European Union rules the world**. 1 ed. Nova Iorque: Oxford University Press, 2020.

BRANCO, P. G. G. Comentário sobre artigo 5º, XVI a XXI. *In*: **Comentários à Constituição do Brasil**. Coordenado por J. J. Gomes Canotilho, Gilmar F. Mendes e Ingo W. Sarlet. São Paulo: Saraiva/Almedina, 2013.

BRASIL. **Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal**. Elaborado pela Comissão de Juristas instituída por Ato do Presidente da Câmara dos Deputados, de 26 nov. 2019. Disponível em: <https://static.poder360.com.br/2020/11/DADOS-Anteprojeto-comissao-protecao-dados-seguranca-persecucao-FINAL.pdf.> Acesso em: 06 out. 2024.

BRANDÃO, C. Teorias da conduta no direito penal. *In*: **Revista de Informação Legislativa**. a. 37 n. 148. Brasília, out.-dez. 2000, pp. 89-95.

BRASIL. CÂMARA DOS DEPUTADOS. **Projeto de Lei n. 21/2020**. Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1853928&filename=PL%2021/2020>. Acesso em: 08 out. 2024.

BRASIL. CÂMARA DOS DEPUTADOS. **Projeto de Lei n. 759/2023**. Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2262557&filename=Avulso%20PL%20759/2023#:~:text=Congresso%20Nacional%20decreta%3A-,Art.,Distrito%20Federal%20e%20dos%20Munic%C3%ADpios.>. Acesso em: 08 out. 2024.

BRASIL. CÂMARA DOS DEPUTADOS. **Projeto de Lei n. 4612/2019b**. Disponível em: <https://bit.ly/3sXGnvT>. Acesso em: 08 out. de 2024.

BRASIL. CÂMARA DOS DEPUTADOS. **Projeto de Lei n. 9736/2018a**. Disponível em: <https://bit.ly/3h6SQbj>. Acesso em: 08 out. 2024.

BRASIL. **Constituição da República Federativa do Brasil**: promulgada em 05 de outubro de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em 02 ago. 2024.

BRASIL. **DECRETO Nº 592, DE 6 DE JULHO DE 1992a**. Atos Internacionais. Pacto Internacional sobre Direitos Civis e Políticos. Promulgação. Disponível em: < https://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d0592.htm>. Acesso em: 02 ago. 2024.

BRASIL. **DECRETO Nº 678, DE 6 DE NOVEMBRO DE 1992b.** Promulga a Convenção Americana sobre Direitos Humanos (Pacto de São José da Costa Rica), de 22 de novembro de 1969. Disponível em: < https://www.planalto.gov.br/ccivil_03/decreto/d0678.htm>. Acesso em: 02 ago. 2024.

BRASIL. **DECRETO-LEI Nº 2.848, DE 7 DE DEZEMBRO DE 1940.** Código Penal. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em: 02 ago. 2024.

BRASIL. **DECRETO-LEI Nº 3.689, DE 3 DE OUTUBRO DE 1941.** Código de Processo Penal. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm>. Acesso em: 02 ago. 2024.

BRASIL. **LEI Nº 6.683, DE 28 DE AGOSTO DE 1979**. Concede anistia e dá outras providências. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l6683.htm>. Acesso em: 02 out. 2024.

BRASIL. **LEI Nº 12.037, DE 1º DE OUTUBRO DE 2009**. Dispõe sobre a identificação criminal do civilmente identificado, regulamentando o art. 5º, inciso LVIII, da Constituição Federal. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2009/lei/l12037.htm>. Acesso em: 02 out. 2024.

BRASIL. **LEI Nº 13.444, DE 11 DE MAIO DE 2017**. Dispõe sobre a Identificação Civil Nacional (ICN). Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13444.htm>. Acesso em: 02 out. 2024.

BRASIL. **LEI Nº 13.709, DE 14 DE AGOSTO DE 2018b**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 12 ago. 2024.

BRASIL. Ministério da Justiça. **Portaria n. º 793, de 24 de outubro de 2019c** Regulamenta o incentivo financeiro das ações do Eixo Enfrentamento à Criminalidade Violenta, no âmbito da Política Nacional de Segurança Pública e Defesa Social e do Sistema Único de Segurança Pública, com os recursos do Fundo Nacional de Segurança Pública, previstos no inciso I do art. 7º da Lei nº 13.756, de 12 de dezembro de 2018. Disponível em: <https://www.gov.br/mj/pt-br/assuntos/sua-seguranca/seguranca-publica/ensino-e-pesquisa/fundo-a-fundo/portaria-no-793-2019-enfrentamento-a-criminalidade-violenta.pdf>. Acesso em: 10 set. 2024.

BRASIL. SENADO FEDERAL. **Projeto de Lei 2.338/2023b**. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=9347593&ts=1726246471801&disposition=inline>. Acesso em: 08 out. 2024.

BRASIL. Superior Tribunal de Justiça. **Agravo Regimental no Agravo em Recurso Especial n. 2.666.044/SP**. Relator Ministro Sebastião Reis Júnior, Sexta Turma, julgado em 27/8/2024, DJe de 2/9/2024. Disponível em: <http://www.stj.jus.br>. Acesso em: 20 ago. 2024.

BRASIL. Superior Tribunal de Justiça. **IDC n. 1/PA,** relator Ministro Arnaldo Esteves Lima, Terceira Seção, julgado em 8/6/2005, DJ de 10/10/2005, p. 217. Disponível em: <http://www.stj.jus.br>. Acesso em: 20 ago. 2024.

BRAYNE, S. **Predict and surveil: data, discretion, and the future of policing**. New York, NY: Oxford University Press, 2021.

BUENO, T. M.; CANAAN, R. G. The Brussels Effect in Brazil: Analysing the impact of the EU digital services act on the discussion surrounding the fake news bill. *In*: **Telecommunications Policy**, n. 48, 2024.

BUOLAMWINI, J.; GEBRU, T. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *In*: **Proceedings of Machine Learning Research**, [s. l.], v. 81, Conference on Fairness, Accountability, and Transparency, 2018, pp. 01-15.

BUONAMICI, S. C. Direito fundamental social à segurança pública. *In*: **Revista de Estudos Jurídicos da UNESP**, Franca, v. 15, n. 21, 2011. DOI: 10.22171/rej.v15i21.341. Disponível em: <https://ojs.franca.unesp.br/index.php/estudosjuridicosunesp/article/view/341>. Acesso em: 21 jan. 2024.

BURRELL, J. How the machine 'thinks': Understanding opacity in machine learning algorithms. *In*: **Big Data & Society**. January–June, 2016, pp. 1–12.

COIMBRA, J. P. M.; MORAES, L. C.; SILVA, A. B. Interseções entre racismo algorítmico, reconhecimento facial e segurança pública no Brasil. *In*: **Revista Jurídica do CESUPA**, v. 4, n. 2, 2023, pp. 136-160.

CONSELHO NACIONAL DE JUSTIÇA. **Justiça em Números 2023**. Conselho Nacional de Justiça, Brasília, 2023.

CORTE INTERAMERICANA DE DIREITOS HUMANOS**. Caso Empregados da Fábrica de Fogos de Santo Antônio de Jesus e seus Familiares vs. Brasil.** Sentença de 15 de julho de 2020.

CORTE INTERAMERICANA DE DIREITOS HUMANOS**. Caso Escher e Outros vs. Brasil.** Sentença de 6 de julho de 2009a.

CORTE INTERAMERICANA DE DIREITOS HUMANOS**. Caso Favela Nova Brasília vs.** Brasil Sentença de 16 de fevereiro de 2017.

CORTE INTERAMERICANA DE DIREITOS HUMANOS**. Caso Garibaldi vs. Brasil** Sentença de 23 de setembro de 2009b.

CORTE INTERAMERICANA DE DIREITOS HUMANOS**. Caso Honorato e Outros vs. Brasil.** Sentença de 27 de novembro de 2023a (exceções preliminares, mérito, reparações e custas) Resumo oficial emitido pela Corte Interamericana. Disponível em: <https://www.gov.br/mdh/pt-br/navegue-por-temas/atuacao-internacional/sentencas-da-corte-interamericana/ResumoSentenaCastelinho.CorteIDH.pdf>. Acesso em: 01 dez. 2024.

CORTE INTERAMERICANA DE DIREITOS HUMANOS**. Caso Tavares Pereira e Outros vs. Brasil.** Sentença de 16 de novembro de 2023b (exceções preliminares, mérito, reparações e custas). Resumo Oficial Emitido pela Corte Interamericana. Disponível em: <https://www.gov.br/mdh/pt-br/navegue-por-temas/atuacao-internacional/sentencas-da-corte-interamericana/ResumodasentenaTavaresPereira.CorteIDH.pdf>. Acesso em: 01 dez. 2024.

CORTE INTERAMERICANA DE DIREITOS HUMANOS**. Caso Trabalhadores Da Fazenda Brasil Verde vs. Brasil**. Sentença de 20 de outubro de 2016.

CORTE INTERAMERICANA DE DIREITOS HUMANOS**. Caso Ximenes Lopes vs. Brasil**. Sentença de 4 de julho de 2006.

COSTA, R.; KREMER, B. Inteligência artificial e discriminação: desafios e perspectivas para a proteção de grupos vulneráveis diante das tecnologias de reconhecimento facial. *In*: **Direitos Fundamentais & Justiça**. Belo Horizonte, ano 16, número especial, out. 2022, pp. 145-167.

DAGUER, B.; BORRI, L. A.; SOARES, R. J. O reconhecimento facial na segurança pública e a proteção de dados pessoais como garantia fundamental. *In*: **Revista de Direito e as Novas Tecnologias**. v. 16, jul.-set. 2022.

DE HERT, P.; BOUCHAGIAR, G. European Biometric Surveillance, Concrete Rules, and Uniform Enforcement. Beyond Regulatory Abstraction and Local Enforcement. *In*: **The Cambridge Handbook of Facial Recognition in the Modern State**. Editado por Rita Matulionyte e Monika Zalnieriute. Cambridge University Press: 2024.

DE PÁDUA, S. R.; LORENZETTO, B. M. O direito fundamental à explicabilidade da inteligência artificial utilizada em decisões estatais. *In*: **Revista da AGU**, *[S. l.]*, v. 23, n. 02, 2024. DOI: 10.25109/2525-328X.v.23.n.02.2024.3480. Disponível em: <https://revistaagu.agu.gov.br/index.php/AGU/article/view/3480>. Acesso em: 7 set. 2024.

DEMERCIAN, P. H. A colaboração premiada e a lei das organizações criminosas. *In*: **Revista Jurídica da Escola Superior do Ministério Público de São Paulo**. ano 5, v. 9, jan.-jun. 2016, pp. 53-88.

DEMERCIAN, P. H.; MORAES, A. R. A. Jurimetria e Inteligência Artificial como ferramentas para uma Política Criminal mais eficiente. *In*: **Inteligência Artifical aplicada ao processo de tomada de decisões**. Coordenado por Henrique Alves Pinto, Jefferson Carús Guedes e Joaquim Portes de Cerqueira César. 1. ed. Belo Horizonte, São Paulo: Editora D´Plácido, 2020, pp. 601-630.

DUARTE, R.; BALDASSO, R. P.; BEUX, L.; ALBERT, A. C. F.; SANTOS, N. C.; FERNANDES, M.M. Aplicação dos Sistemas Biométricos de Reconhecimento Facial na Segurança Pública. *In*: **Brazilian Journal of Forensic Sciences, Medical Law and Bioethics** 11(1), 2021, pp. 1-21.

DUBAL, V. San Francisco was rightto ban facialrecognition. Surveillance is a real Danger. *In*: **The Guardian**. 30/05/2019. Disponível em: <https://www.theguardian.com/commentisfree/2019/may/30/san-francisco-ban-facial-recognition-surveillance#:~:text=Surveillance%20is%20a%20real%20danger,-This%20article%20is&text=San%20Francisco's%20recent%20municipal,agencies%20has%20received%20international%20attention.>. Acesso em: 08 set. 2024.

DUSHI, D. The use of facial recognition technology in EU law enforcement: Fundamental rights implications. *In*: **Policy Briefs 2020**. Global Campus South East Europe, 2020.

EBERS, M.; HOCH, V. R. S.; ROSENKRANZ, F.; RUSCHEMEIER, H.; STEINRÖTTER, B. The European Commission's Proposal for an Artificial Intelligence Act - A Critical Assessment by Members of the Robotics and AI Law Society (RAILS). *In*: **Multidisciplinary Scientific Journal**. 2021, pp. 589–603. Disponível em: <https://doi.org/10.3390/j4040043.>. Acesso em: 24 set. 2024.

ERTHAL, C. N. A. **A segurança pública como direito fundamental e como tarefa estatal na Constituição brasileira de 1988. Dissertação do Mestrado em Direito e Ciência Jurídica**. Especialidade em Direitos Fundamentais, Universidade de Lisboa, 2020. Disponível em: <https://repositorio.ul.pt/handle/10451/48042>. Acesso em: 21 jan. 2024.

EU ARTIFICIAL INTELLIGENCE ACT. **Historic Timeline**. Sítio eletrônico mantido pelo Future of Life Institute (FLI). Disponível em: <https://artificialintelligenceact.eu/developments/>. Acesso em: 10 ago. 2024.

FARIA, R. B.; SILVA, R. G. M. Breves considerações acerca da utilização do reconhecimento facial como instrumento de segurança pública e persecução. *In*: **Boletim IBCCRIM**, 31(362), 2023, pp. 14–17, disponível em: <https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/1561>. Acesso em: 26 set. 2024.

FERNANDES, B. G. **Curso de Direito Constitucional**. 10. ed., JusPODIVM: Salvador, 2018.

FERRAJOLI, L. **Por uma constituição da Terra**: a humanidade em uma encruzilhada. Tradução por Sergio Cademartori e Jesus Tupã Silveira Gomes. 1. ed., Florianópolis: Emais, 2023.

FIORDI, L. COWLS, J.; BELTRAMETTI, M.; CHATILA, R.; CHAZERAND, P.; DIGNUM, V.; LÜTGE, C; MADELIN, R.; PAGALLO; U.; ROSSI, F.; CHAFER, B.; VALCKE, P.; VAYENA, E. AI4People. An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations. *In*: **Minds and Machines**, 28, 2018 pp. 689–707.

FISCHER, D.; PEREIRA, F. V.. **As obrigações processuais penais positivas**: segundo as Cortes Europeia e Interamericana de Direitos Humanos. 4. ed. rev. atual. e ampl. com as 11 condenações do Brasil na Corte IDH e as Recomendações 123/2022 do CNJ e 96/2023 do CNMP. Porto Alegre: Livraria do Advogado, 2023.

FONTES, C.; HOHMA, E.; CORRIGAN, C. C.; LÜTGE, C. AI-powered public surveillance systems: why we (might) need them and how we want them. *In*: **Technology in Society**. Elsevier, 2022, pp. 02-37.

FONTES, C; PERRONE, C. Ethics of surveillance: harnessing the use of live facial recognition technologies in public spaces for law enforcement. *In*: **Institute for Ethics in Artificial Intelligence, Research Brief**. Technical University of Munich, 2021.

FRA - EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS. **Facial recognition technology: fundamental rights considerations in the context of law enforcement**. Publications Office of the European Union: European Union Agency for Fundamental Rights, 2020.

FRANKEL, C.; GALLAND, J. **Market, regulation, market, regulation**. Apresentado na 20th EURAS Annual Standardization Conference, EURAS, Copenhagen, Denmark, jun. 2015.

FREITAS, J. **Direito Fundamental À Boa Administração Pública**. 3ª Edição. São Paulo: Malheiros Editores, 2014.

GANS-COMBE, C. Automated Justice: Issues, Benefits and Risks in the Use of Artificial Intelligence and Its Algorithms in Access to Justice and Law Enforcement. *In*: **Ethics, Integrity and Policymaking The Value of the Case Study**. Editores: Dónal O'Mathúna e Ron Iphofen. Springer, 2022.

GOLDENFEIN, J. Privacy's Loose Grip on Facial Recognition *Law and the Operational Image. In*: **The Cambridge Handbook of Facial Recognition in the Modern State**. Editado por Rita Matulionyte e Monika Zalnieriute. Cambridge University Press, 2024.

GOODFELLOW, I.; BENGIO, Y.; COURVILLE, A. **Deep Learning**. Cambridge, MA: MIT Press, 2016.

GRINBERG, F., ARAÚJO, V., FREITAS, H., RIBEIRO, A. **Prisões por reconhecimento facial avançam pelo país, mas erros em série desafiam tecnologia de combate ao crime**. O Globo, Rio de Janeiro e São Paulo, 05 jan. 2024. Disponível em: <https://oglobo.globo.com/brasil/noticia/2024/01/05/prisoes-por-reconhecimento-facial-avancam-pelo-pais-mas-erros-em-serie-desafiam-tecnologia-de-combate-ao-crime.ghtml>. Acesso em: 28 abr. 2024.

GÜLTEKIN-VÁRKONYI, G. Predictive Policing and Bias in a Nutshell: Technical and Practical Aspects of Personal Data Processing for Law Enforcement Purposes. *In*: **Digital Criminal Justice**: A Studybook Selected Topics for Learners and Researchers. Krisztina Karsai, Adem Sözüer, Liane Wörner (eds.). Istanbul, 2022.

HIROSE, M., "Privacy in Public Spaces: The Reasonable Expectation of Privacy against the Dragnet Use of Facial Recognition Technology". *In*: **Connecticut Law Review**. v. 49, n. 5, set. 2017, pp. 1593-1620.

HOFFMANN-RIEM, W. Big data e inteligência artificial: desafios para o direito. Tradução pelos Professores Doutores, Gabrielle Bezerra Sales Sarlet e Carlos Alberto Molinaro. Revisão do Prof. Dr. Ingo Wolfgang Sarlet. *In*: Journal of Institutional Studies 2 (2020) **Revista Estudos Institucionais**, v. 6, n. 2, mai-.ago. 2020, pp. 431-506.

INSTITUTO NACIONAL DE METROLOGIA, QUALIDADE E TECNOLOGIA. **Estudo sobre os modelos regulatórios da Europa e dos Estados Unidos da América, e sobre a influência da indústria 4.0 na modernização da regulamentação do Inmetro**. Coordenação por Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH. Diretor Nacional Michael Rosenauer. Grupo de Trabalho para assessorar o Presidente na Modernização do Modelo Regulatório do Inmetro (GTMRI), por intermédio da Portaria Inmetro nº 212/2020.

INSTITUTO IGARAPÉ. **Infográfico: Reconhecimento facial no Brasil**. Disponível em: <https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/>. Acesso em: 15 dez. 2024.

INTRONA, L. D.; NISSENBAUM, H. **Facial Recognition Technology A Survey of Policy and Implementation Issues**. UK: Lancaster University Management School, 2010.

INTRONA, L. D; WOOD, D. Picturing Algorithmic Surveillance: The Politics of Facial Recognition Systems. *In*: **Surveillance & Society CCTV Special** (eds. Norris, McCahill and Wood) 2(2/3), 2004, pp. 177-198.

KHAN, Z. A.; RIZVI, A. AI based facial recognition technology and criminal justice: issues and challenges. *In*: **Turkish Journal of Computer and Mathematics Education,** v.12, n.14, 2021, pp. 3384-3392.

KRIEBITZ, A.; LÜTGE, C. Artificial Intelligence and Human Rights: A Business Ethical Assessment. *In*: **Business and Human Rights Journal**, fev. 2020.

KUHLMANN, S. Government Use of Facial Recognition Technologies under European Law. *In*: **The Cambridge Handbook of Facial Recognition in the Modern State**. Editado por Rita Matulionyte e Monika Zalnieriute. Cambridge University Press, 2024.

LAZZARINI, A. Da segurança pública na Constituição de 1988. *In*: **Revista de Informação Legislativa**. Brasília, a. 26, n. 104, out.-dez. 1989.

LOPES JR. A. **Direito Processual Penal**. 10 ed. São Paulo: Saraiva: 2013.

LORENZON, L. N. AAnálise comparada entre regulamentações de dados pessoais no Brasil e na União Europeia (LGPD e GDPR) e seus respectivos instrumentos de enforcement. *In*: **Revista do Programa de Direito da União Europeia**, v. 1. FGV, 2021.

LYNCH, N. Facial Recognition Technology in Policing and Security, Case Studies. *In*: **Regulation. Laws** 13, 35, 2024. Disponível em: < https:// doi.org/10.3390/laws13030035>. Acesso em: 25 jul. 2024.

LYNCH, N.; CAMPBELL, L. Principled Regulation of Facial Recognition Technology: A View from Australia and New Zealand. *In*: **The Cambridge Handbook of Facial Recognition in the Modern State**. Editado por Rita Matulionyte e Monika Zalnieriute. Cambridge University Press, 2024.

MADIEGA, T. **Artificial Intelligence Act**, EPRS, European Parliament, mar. 2024.

MAGALHÃES, A. A.; GOMES, T. S. Regulação de sistemas de reconhecimento facial para fins de segurança pública no Brasil: riscos e desafios. *In*: **Revista Humanidades e Inovação** v. 8, n. 47, 2021, pp. 168-182.

MATULIONYTE, R. Transparency of Facial Recognition Technology and Trade Secrets. *In*: **The Cambridge Handbook of Facial Recognition in the Modern State**. Editado por Rita Matulionyte e Monika Zalnieriute. Cambridge University Press, 2024.

MCCARTHY, J.; MINSKY, M. L.; ROCHESTER, N.; SHANNON, C. E. A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence August 31, 1955. *In*: **AI Magazine**, v. 27, n. 4, 2006, pp. 12-14.

MCKENDRICK, K. Artificial Intelligence Prediction and Counterterrorism. *In*: **International Security Department**, The Royal Institute of International Affairs Chatham House, August, 2019.

MELO, P. V.; SERRA, P. Tecnologia de Reconhecimento Facial e Segurança Pública nas Capitais Brasileiras: Apontamentos e Problematizações. *In*: **Comunicação e Sociedade**, v. 42, 2022, pp. 205-220.

MENDES, G. F.; BRANCO, P. G. G. **Curso de direito constitucional**. 7. ed. rev. e atual. São Paulo: Saraiva, 2012.

MOBILIO, G. Your face is not new to me – Regulating the surveillance power of facial recognition Technologies. *In*: **Internet Policy Review** – Journal on internet regulation. v. 12. issue 1, 2023.

MORAES, A. **Direito Constitucional**. 24ª edição. São Paulo: Atlas, 2009.

MORAES, A. R. A. **Direito penal racional**: propostas para a construção de uma teoria da legislação e para uma atuação criminal preventiva. Curitiba: Juruá, 2016.

MORAES, A. R. A.; DEMERCIAN, P. H. Um novo modelo de atuação criminal para o Ministério Público brasileiro: agências e laboratório de jurimetria. *In*: **Revista Jurídica ESMP-SP**, v. 11, 2017, p.14 – 40.

MORAES, A. R. A; LISBOA, A. F. Regulamentação da Inteligência Artificial na União Europeia: estrutura ética, classificação de riscos e possíveis reflexos na medicina. *In*: **UNISANTA Law and Social Science**, v. 13, n. 2, 2024, pp. 16-29.

MOREIRA NETO, D. F. A Segurança Pública na Constituição. *In*: **O Alferes**, v. 9 n. 28. Belo Horizonte: jan.-mar., 1991, pp. 11-23.

NAJIBI, A. Racial Discrimination in Face Recognition Technology. *In*: Science in the News. October, 24. 2020. Disponível em: <https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/>. Acesso em: 18 abr. 2023.

OECD - Organisation for Economic Co-operation and Development. **Artificial Intelligence in Society**. OECD Publishing: Paris, 2019.

OLIVEIRA, K. D. **Processo penal convencional e fundamentos das obrigações processuais penais positivas do estado em matéria penal**. 1ª edição. Belo Horizonte, São Paulo: D'Placido, 2022.

OLIVEIRA, L.V.; CRIPPA, M. E. N; LAURENTE, I; HOLANDA, T. Aspectos ético-jurídicos e tecnológicos do emprego de reconhecimento facial na segurança pública no Brasil. *In*: **Revista Tecnologia e Sociedade**. Curitiba, v. 18, n. 50, p.114-135, jan.-mar., 2022. Disponível em: <https://periodicos.utfpr.edu.br/rts/article/view/12968>. Acesso em: 05 ago. 2024.

OLIVEIRA, S. A. M. A teoria geracional dos direitos do homem na filosofia de Norberto Bobbio. *In*: SALATINI, R.; BARREIRA, C. M. **Democracia e direitos humanos no pensamento de Norberto Bobbio**. Marília: Oficina Universitária; São Paulo: Cultura Acadêmica, 2018. p. 247-262.

ORTIGOSA, A. P. Quién es quién en el Reglamento Europeo de inteligencia artificial? Las autoridades notificantes y los organismos notificados. *In*: **Actualidad Jurídica Iberoamericana**, n. 21, ago. 2024, pp. 598-617.

PASQUINELLI, M. How a machine learns and fails. *In*: **Spheres**, Journal for Digital Cultures. #5 Spectres of AI, 2019, pp. 1–17.

PELE, A.; MULHOLLAND, C. On Facial Recognition, Regulation, and "Data Necropolitics". *In*: **Indiana Journal of Global Legal Studies**, Published by Indiana University. Press. v. 30, issue 1, 2023, pp. 173-194.

PEREIRA, R. S. 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 inteligência artificial. *In*: **Revista da Faculdade de Direito da Universidade de Lisboa**. Número Temático: Tecnologia e Direito. v. LXIII, números 1 e 2, 2022, pp. 839-865.

PORTUGAL. **Decreto-Lei n.º 48/95**. Código Penal. Diário da República n.º 63/1995, Série I-A de 1995-03-15. Disponível em: <https://diariodarepublica.pt/dr/legislacao-consolidada/decreto-lei/1995-34437675>. Acesso em: 01 set. 2024.

PORTUGAL. **Lei n.º 52/2003, de 22 de Agosto**. LEI DE COMBATE AO TERRORISMO. Disponível em: <https://diariodarepublica.pt/dr/detalhe/lei/52-2003-656128>. Acesso em 01 de setembro de 2024.

PRADO, L. R.; CARVALHO, E. M.; CARVALHO, G. M. **Curso de direito penal brasileiro**. 14 ed., São Paulo: Editora Revista dos Tribunais, 2015.

RAJI, I. D.; GEBRU, T.; MITCHELL, M; BUOLAMWINI, J.; LEE, J.; DENTON, E. Saving Face: Investigating the Ethical Concerns of Facial Recognition Auditing. *In*: **AIES '20**, New York, NY, USA, February 7–8, 2020, pp. 145-151.

RAMOS, A. C. **Curso de Direitos Humanos**. 11. ed. São Paulo: Saraiva Jur, 2024. ePUB.

RAPOSO, V. L. The Use of Facial Recognition Technology by Law Enforcement in Europe: a Non-Orwellian Draft Proposal. *In*: **European Journal on Criminal Policy and Research** 29. Springer: 2023, pp. 515–533.

RASO, F. A.; HILLIGOSS, H.; KRISHNAMURTHY, V.; BAVITZ, C.; KIM, L. **Artificial Intelligence & Human Rights: Opportunities & Risks**. Berman Klein Center – For Internet & Society At Harvard University: 2018. Disponível em: <https://cyber.harvard.edu/publication/2018/artificial-intelligence-human-rights>. Acesso em: 04 ago. 2024.

RIOS. R. R.; SILVA. R. Discriminação múltipla e discriminação interseccional: aportes do feminismo negro e do direito da antidiscriminação. *In*: **Revista Brasileira de Ciência Política**, nº16. Brasília, jan.-abr. 2015, pp. 11-37.

ROLA, E. C. S. **Os principais contributos da inteligência artificial para o processamento de imagens digitais a utilizar na segurança pública**. Dissertação do Mestrado em Segurança

e Justiça, orientada por Prof. Doutor Luís Carlos Rodrigues Malheiro. Universidade Lusíada, 2022.

RODRIGUES, E. B. The Brussels Effect. Em: BRADFORD, Anu. The Brussels effect: how the European Union rules the world. 1 ed. Nova Iorque: Oxford University Press, 2020. p. 25-65. **Scientia Iuris**, Londrina, v. 25, n. 2, jul. 2021, pp. 205-207.

RODRIGUES, J. G. Lineamentos sobre a nova dinâmica resolutiva do Ministério Público. *In*: **Revista Jurídica ESMP-SP**, v.8, 2015, pp. 53-90.

ROTSCH. T. Criminal Compliance. In: **InDret - Revista Para el Análisis del Derecho**. Tradução por Ivó Coca Vila, Universidad Pompeu Fabra. Revisão pelo Prof. Dr. Ricardo Robles Planas. Barcelona, jan. 2012, pp. 1-11.

RUSCHEMEIER, H. AI as a challenge for legal regulation – the scope of application of the artificial intelligence act proposal. *In*: **ERA Forum.** Springer Nature: 2023, pp. 361–376.

SAAVEDRA, G. A. Compliance criminal: revisão teórica e esboço de uma delimitação conceitual. *In*: **Revista Duc In Altum**, Cadernos de Direito, v. 8, n .15, mai.-ago. 2016, pp. 239-256.

SADEK, M. T. A construção de um novo Ministério Público resolutivo. *In*: **De jure: Revista jurídica do Ministério Público do Estado de Minas Gerais**, Belo Horizonte, n. 12, 2009.

SANTOS, J. G. Reconhecimento facial: entre a criminologia, a mídia e a LGPD penal. *In*: **Internet & Sociedade**. v. 2, n. 1, jun. 2021, pp. 214-232.

SANTOS, M. C. C. L.; ARAÚJO, M. Arquiteturas digitais: consequências das novas tecnologias nos direitos das vítimas. *In*: **Revista de Vitimologia e Justiça Restaurativa**, ano I, v. II, jul. 2023, pp. 61-84.

SARLET, I. W. Teoria geral dos direitos fundamentais. *In*: **Curso de Direito Constitucional** / Ingo Wolfgang Sarlet, Luiz Guilherme Marinoni, Daniel Mitidiero. 11. ed., São Paulo: SaraivaJur, 2022.

SARLET, I. W. Notas introdutórias ao sistema constitucional de direitos e deveres fundamentais. *In*: **Comentários à Constituição do Brasil**. Coordenado por J. J. Gomes Canotilho, Gilmar F. Mendes e Ingo W. Sarlet. São Paulo: Saraiva/Almedina, 2013.

SELINGER, E; HARTZOG, W. The Inconsentability of Facial Surveillance. *In*: **Loyola Law Review**, 2019. Disponível em: <https://scholarship.law.bu.edu/faculty_scholarship/3066>. Acesso em: 30 jun. 2024.

SELWYN, N; ANDREJEVIC, M; O´NEILL, C. GU, X. SMITH, G. Facial Recognition Technology Key Issues and Emerging Concerns. *In*: **The Cambridge Handbook of Facial Recognition in the Modern State**. Editado por Rita Matulionyte e Monika Zalnieriute. Cambridge University Press, 2024.

SIEGMANN, C.; ANDERLJUNG, M. **The Brussels Effect and Artificial Intelligence: How EU regulation will impact the global AI market**. Centre for the Governance of AI. ago. 2024.

SILVA, D. C.; ANDREA, G. F. M.; GUNDIM, W. W. D. Tecnologia de reconhecimento facial como política de segurança pública: o caso do metrô de São Paulo: O CASO DO METRÔ DE SÃO PAULO. *In*: **Revista da Faculdade de Direito do Sul de Minas**, Pouso Alegre, v. 38, n. 2, jul.-dez. 2022, pp. 279-298.

SMITH, M; MANN, M. Facial Recognition Technology and Potential for Bias and Discrimination. *In*: **The Cambridge Handbook of Facial Recognition in the Modern State**. Editado por Rita Matulionyte e Monika Zalnieriute. Cambridge University Press, 2024.

SMITH, M; MILLER, S. The ethical application of biometric facial recognition technology. *In*: **AI & Society**, 37, 2022, pp.167–175.

SMUHA, N; AHMED-RENGERS, E.; HARKENS, A.; LI, W.; MACLAREN, J.; PISELLI, R.; YEUNG, K. **How the EU can achieve legally trustworthy AI: a response to the European Commission's Proposal for an Artificial Intelligence Act**. Leads Lab @ University of Birmingham: 2021.

SOUSA, B.; FICO, B. S. D.; MARANHÃO, J. S. A.; NAVAS, J. M. M. S.; BUZONE, J. P. N; BARROS, J. M.; ALMADA, M. **Efeito Bruxelas: concepção, processos e influência do Direito da União Europeia**. São Paulo: Maranhão & Menezes Advogados Associados, 2024.

SOUZA, M. C.; JÚNIOR, W. J. V. GLOBALIZAÇÃO E DIREITO HUMANO CULTURAL. *In*: **Edição Extraordinária - Direitos Humanos**, v. 1 n. 1-Ext, 2019, pp. 86-103.

SOUZA NETO, C. P. Comentário sobre o direito à segurança. *In*: **Comentários à Constituição do Brasil**. Coordenado por J. J. Gomes Canotilho, Gilmar F. Mendes e Ingo W. Sarlet. São Paulo: Saraiva/Almedina, 2013.

TAYOR, S. M. FRT in 'Bloom' Beyond Single Origin Narratives. *In*: **The Cambridge Handbook of Facial Recognition in the Modern State**. Editado Rita Matulionyte e Monika Zalnieriute. Cambridge University Press, 2024.

TELEFI, Project. **Summary Report of the project "Towards the European Level Exchange of Facial Images"**. Fundado por European Union Internal Security Fund-Police. v. 1.0, jan. 2021.

UNIÃO EUROPEIA. **Guia Azul de 2016 sobre a Aplicação das Regras da UE em matéria de Produtos**. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:JOC_2016_272_R_0001&from=PT>. Acesso em 11 set. 2024.

UNIÃO EUROPEIA. **Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024 que cria regras harmonizadas em matéria de inteligência artificial e que altera os Regulamentos (CE) n.o 300/2008, (UE) n.o 167/2013, (UE) n.o 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e as Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regulamento da Inteligência Artificial)**. Publicado no Jornal Oficial da União Europeia em 12 de julho de 2024. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689>. Acesso em: 01 ago. 2024.

URQUHART, L.; MIRANDA, D. Policing faces: the present and future of intelligent facial surveillance, *In*: **Information & Communications Technology Law**, v. 31. n. 02. 2022, pp. 194-219.

VARGAS, E. N. P.; RIBEIRO, M. M. Reconhecimento facial como política de segurança pública no estado da Bahia. *In*: **Terceiro Milênio: Revista Crítica de Sociologia e Política** v. 22, n. 3, set.-dez. 2023, pp. 190-216.

VICHEVA, M.; MITOVA, M. Role of Standardisation for Developing Single European Market. *In*: **14th International Conference in "Standardization, protypes and quality: a means of balkan countries' collaboration"**, Tirana, Albania, set. 21 - 22, 2018, pp. 298-306.

WIEK, K. The Artificial Intelligence Act. **The Impact of AI on Human Rights Standards in European Law Enforcement.** Bachelor Thesis, orientada por Dr. C. Matera. University of Twente, Enschede, NL, 2023.

WINFIELD, A. F. T; JIROTKA, M. Ethical governance is essential to building trust in robotics and artificial intelligence systems. *In*: **Philosophuical Transactions of the Royal Society A**. v. 376, issue 2133, 2018.

WU, H; ALBIERO, V.; KRISHNAPRIYA, K. S.; KING, M. C., BOWYER, K. W. Face Recognition Accuracy Across Demographics: Shining a Light Into the Problem. *In*: **IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW).** 2023, pp. 1041-1050.

ZALNIERIUTE, M. Power and Protest: Facial Recognition and Public Space Surveillance. *In*: **The Cambridge Handbook of Facial Recognition in the Modern State**. Editado por Rita Matulionyte e Monika Zalnieriute. Cambridge University Press, 2024.

ZENKNER, M. Corregedoria e efetividade do Ministério Público: a necessidade de revisitar a atuação demandista. *In*: **Revista Jurídica da Corregedoria Nacional do Ministério Público: o papel constitucional das Corregedorias do Ministério Público**, v.1. Brasília: CNMP, 2016, p. 203-216.

ZHAROVA, A.; ELIN, V.; PANFILOV, P. Introducing Artificial Intelligence into Law Enforcement Practice: The Case of Russia. *In*: **Proceedings of the 30th DAAAM International Symposium**, pp.0688-0692, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734-22-8, ISSN 1726-9679, Vienna, Austria, 2019.