https://doi.org/10.54795/rejub.n.1.186

A UTILIZAÇÃO DO RECONHECIMENTO FACIAL COMO INSTRUMENTO DE COMBATE AO CRIME ORGANIZADO TRANSNACIONAL E AO TERRORISMO: LIMITES E PERSPECTIVAS

THE USE OF FACIAL RECOGNITION AS A INSTRUMENT TO FIGHT TRANSNATIONAL ORGANIZED CRIME AND TERRORISM: LIMITS AND PERSPECTIVES

FABIO NUNES DE MARTINO
Graduado em Direito pela Universidade Federal do Estado do Rio de Janeiro (2000). Especialista em Direito Penal e Criminologia pela Pontifícia Universidade Católica do Rio Grande do Sul – PUC/RS (2020). Mestre em Justiça Administrativa pela Universidade Federal Fluminense (2021) e mestrando em Direito Processual pela Universidade de São Paulo. Atualmente é juiz federal – Seção Judiciária do Paraná.
https://orcid.org/0000-0003-1561-9976

RESUMO

Para enfrentar os desafios gerados pela constante atuação do crime organizado transnacional e das organizações terroristas, os estados se viram obrigados a utilizar novos mecanismos de investigação com o objetivo de tornar mais eficiente a atividade de prevenção e de repressão a esses delitos. Entre os mecanismos, encontra-se o reconhecimento facial automatizado. Partindo desse contexto, este artigo pretende fazer uma análise da utilização dessa tecnologia como ferramenta voltada ao apoio das agências de investigação na prevenção e na repressão da criminalidade organizada e do terrorismo internacional, incluindo uma abordagem sobre a existência de limites técnicos, práticos e jurídicos, bem como expondo as perspectivas para a compatibilização do uso dessa ferramenta de investigação com a proteção dos direitos fundamentais dos indivíduos.

Palavras-chave: reconhecimento facial; eficiência; limites; direitos fundamentais; cooperação judicial internacional.

ABSTRACT

In order to face the challenges generated by the constant activity of transnational organized crime and terrorist organizations, States were forced to use new investigative mechanisms with the objective of making the activity of preventing and repressing these crimes more efficient. Among these mechanisms is automated facial recognition. Based on this context, this article intends to analyze the use of this technology as a tool aimed at supporting investigative agencies in the prevention and repression of organized crime and international terrorism, including an approach to the existence of technical, practical and legal limits, as well as exposing the perspectives for making the use of this research tool compatible with the protection of the fundamental rights of individuals.

Keywords: facial recognition; efficiency; limits; fundamental rights; international judicial cooperation.

Recebido: 13-3-2022
Aprovado: 28-4-2022

SUMÁRIO

fundamentais? 7 Perspectivas e caminhos para o uso eficiente do reconhecimento facial. 8 Conclusão. Referências.

1 INTRODUÇÃO

Diante da evolução das práticas criminosas transnacionais e do terrorismo nas últimas décadas, os países se viram obrigados a aprimorar as estratégias de combate a essas organizações criminosas, incluindo a utilização de novas tecnologias de investigação e, também, o aperfeiçoamento da cooperação internacional entre as agências de persecução penal.

Nesse contexto, o presente artigo objetiva analisar a utilização da tecnologia do reconhecimento facial automatizado como ferramenta voltada ao apoio das agências de investigação na prevenção e na repressão da criminalidade organizada e do terrorismo internacional, incluindo uma abordagem sobre a existência de limites técnicos, práticos e jurídicos, bem como as perspectivas para a compatibilização do uso dessa ferramenta de investigação com a proteção dos direitos fundamentais dos indivíduos.

Para alcançar esse objetivo, inicialmente será exposto um panorama sobre a evolução do combate ao crime organizado transnacional e do terrorismo através da implementação de novas técnicas de investigação e do aperfeiçoamento da cooperação internacional entre as nações.

Na sequência, serão aprofundados os conceitos e as possibilidades de utilização desse mecanismo de identificação biométrica na prevenção e repressão da criminalidade organizada.

Partindo dessa exposição geral sobre o funcionamento do reconhecimento facial voltado para o auxílio à segurança pública, o artigo buscará traçar limitações técnicas, práticas e jurídicas à implementação dessa tecnologia.

No que se refere aos limites técnicos, com base em pesquisas de campo e científicas, serão abordadas as dificuldades dessa ferramenta na correta identificação dos indivíduos, incluindo as limitações decorrentes da má qualidade da imagem captada e, também, os vieses raciais e de gênero que decorrem de falhas relacionadas à programação dos algoritmos ou mesmo ao seu treinamento falho.

No capítulo referente aos limites práticos, serão abordados os requisitos necessários para que essa tecnologia possa ser utilizada de forma eficiente no combate ao crime organizado transnacional e ao terrorismo. Esses requisitos abrangem, por um lado, a necessidade da existência de um banco de dados completo que contenha o maior número possível de padrões faciais arquivados e, também, que haja efetiva integração entre as agências de persecução penal de forma que as informações sejam compartilhadas sem maiores burocracias, mas com respeito à proteção dos dados sensíveis.

O terceiro bloco de limitações abordado pelo texto se refere às limitações jurídicas. Nesse bloco, serão ponderadas relevantes preocupações externadas por vários estudiosos do assunto no sentido de que o reconhecimento facial tem grande potencial de colocar em risco os direitos fundamentais dos cidadãos.

Em seguida, tendo sedimentado as principais críticas feitas com relação à tecnologia, será exposto um panorama atual sobre a utilização do reconhecimento facial automatizado para fins de segurança pública no Brasil e no mundo, incluindo o debate sobre o seu banimento ou

seu uso com limites estritos. Serão ainda delimitados caminhos para o melhor uso dessa relevante ferramenta para investigações criminais, incluindo a necessidade de aprimoramento técnico dos programas, a fixação de limites legais que possibilitem o controle na utilização da tecnologia e, também, a necessidade de aperfeiçoamento da legislação brasileira de proteção e transferência de dados na seara penal, de forma que eleve os *standards* de proteção de dados e, assim, compatibilize-se com legislações estrangeiras mais evoluídas sobre o assunto.

Por fim, a conclusão de forma sintética fará um apanhado das dificuldades e dos caminhos propostos pelo estudo, sempre com o objetivo de compatibilizar a utilização de novas tecnologias de investigação com a proteção dos direitos fundamentais dos cidadãos.

2 A EVOLUÇÃO DO COMBATE AO CRIME ORGANIZADO TRANSNACIONAL E AO TERRORISMO OPERADA ATRAVÉS DO APRIMORAMENTO DA COOPERAÇÃO INTERNACIONAL E DA IMPLEMENTAÇÃO DE NOVAS TECNOLOGIAS DE INVESTIGAÇÃO

A intensificação do fenômeno da globalização nas últimas décadas fez com que fossem derrubadas fronteiras geográficas, sociais, culturais, políticas e econômicas entre pessoas e instituições, modificando por completo as relações internacionais. Esse fenômeno, em grande parte, viu-se estimulado pelos avanços tecnológicos nas áreas das comunicações e da informática, bem como pela evolução dos meios de transporte de longa distância, fatores esses que conjuntamente permitiram o desaparecimento da distância e do tempo em diversas áreas da atividade humana (ZAVASCKI, 2010, p. 9).

Dentro dessa nova realidade mundial, Valente (2013, p. 75) defende que toda essa mudança fez com que os cidadãos deixassem de se sentir vinculados espacialmente a uma sociedade específica, para que cada vez mais passassem a se sentir como integrantes de um todo – ou, em outras palavras, "o viver de cada cidadão é, cada vez mais, um viver como cidadão do mundo".

Esse novo formato do globo também transformou a dinâmica dos crimes que deixaram de ser apenas locais para se transformarem em regionais ou mesmo internacionais (VALENTE, 2013, p. 76) e passassem a afetar bens jurídicos transindividuais, dentre os quais se incluem o meio ambiente, a segurança pública, o sistema financeiro e a ordem econômica (ANDREATO, 2016, p. 147).

Até os crimes mais simples acabam ganhando um contorno internacional. Para isso basta que se imagine que um crime ocorrido no Brasil e que seja praticado por brasileiros contra brasileiros pode exigir para a sua resolução que as autoridades de persecução penal brasileiras acessem dados que estejam localizados no exterior (VIOLA; HERINGER; CARVALHO, 2021, p. 2), o que demonstra que atualmente os dados pessoais transitam naturalmente por todo o mundo sem maiores limitações pela divisão territorial existente.

Observa-se que todas essas mudanças que ocorreram em escala global, e foram benéficas em diversos campos da sociedade, também favoreceram o crime organizado, que se aproveitou da globalização para expandir os seus negócios, que deixaram de ser regionais para alcançarem uma escala mundial (SAADI, 2016, p. 141).

A globalização também modificou a dinâmica do crime de terrorismo que inicialmente se vinculava a movimentos clandestinos locais com o objetivo de libertação nacional e passaram a ser

internacionalizados, afetando por muitas vezes a paz e a segurança das nações (SOUZA, 2016, p. 164). Inclusive, esse fenômeno passou a ser alvo de maiores preocupações dos estados a partir de atentados contra a vida de pessoas indeterminadas, tendo o seu ápice com o atentado das Torres Gêmeas em 11 de setembro de 2001 (VALENTE, 2013, p. 85).

Toda essa expansão da criminalidade organizada e do terrorismo internacional exigiu que os estados fossem obrigados a aperfeiçoar as formas de cooperação e, também, que novas medidas investigativas passassem a ser utilizadas com o objetivo de enfrentar o grande desafio.

No que diz respeito ao aperfeiçoamento da cooperação internacional, verifica-se que, em resposta a essa nova criminalidade que surgiu a partir da globalização mundial, tornou-se necessária a implementação de acordos internacionais de auxílio mútuo em matéria penal em substituição às tradicionais formas de cooperação que utilizam das vias diplomáticas e das autoridades centrais. Assim, a cooperação direta entre os estados se mostrou um relevante instrumento de aproximação entre os diversos órgãos de persecução penal (LESSA, 2016, p. 117).

Diariamente, novos acordos, bilaterais ou multilaterais, disciplinando a cooperação jurídica internacional em matéria penal, são celebrados, o que diminui a utilização das cartas rogatórias e agiliza a efetivação da cooperação entre os países (ANDREATO, 2016, p. 149).

Ao tratar do combate ao terrorismo internacional, Valente (2013, p. 76-78, 90) defende que a cooperação multilateral ou bilateral é fundamental para prevenir atos terroristas ou para identificar os seus autores, desde que respeitada toda a legislação vigente. O autor ainda

sustenta que mais do que uma cooperação judicial entre as nações, deveriam ser criados espaços supranacionais em que se pudesse dar uma resposta tanto no âmbito do Direito Penal Material como no âmbito do Processo Penal.

Diante desse cenário, atualmente existem duas formas principais de cooperação entre as nações: através da inteligência policial e da cooperação jurídica internacional. As cooperações realizadas pelos estados mediante a inteligência policial podem se dar por intermédio das polícias[1], dos ministérios públicos ou mesmo por unidades de inteligência financeira. Já as medidas que demandam análise pelo Poder Judiciário devem se utilizar dos mecanismos da cooperação jurídica internacional (SAADI, 2016, p. 142-143).

Diante de uma realidade permeada por uma descomunal quantidade de dados disponíveis, torna-se muito importante a atividade de inteligência dos estados, visto que é necessário o processamento desses dados para que sejam possíveis as tomadas de decisão, especialmente aquelas preditivas que permitam uma atuação antecipada por parte do Estado (ALVES, 2018, p. 1-6).

Dentro da cooperação jurídica internacional, houve uma evolução com o passar dos anos em que se buscou formas menos burocratizadas de cooperação, especialmente retirando-se qualquer participação política desse processo que, nesse novo formato, privilegia a cooperação direta entre os órgãos de persecução penal dos estados envolvidos.

[1] Por exemplo, através da Interpol ou das adidâncias existentes em diversos países.

Zavascki (2010, p. 10) bem dimensiona a questão:

> Nesta área, a agilidade das condutas ilícitas e a eficácia transnacional de seus resultados se mostravam diretamente proporcionais à ineficiência e à insuficiência dos antigos e tradicionais mecanismos de cooperação utilizados entre os estados, visando combatê-las, consistentes em instrumentos formais e burocratizados, em geral intermediados por órgãos do Judiciário de cada país. Por isso mesmo, inúmeros acordos e tratados celebrados em tempos recentes, em âmbito bilateral e multilateral, dos quais o Brasil também é signatário, buscaram instituir um novo padrão de cooperação, mediante criação de instrumentos mais compatíveis com as exigências dos novos tempos. Construiu-se, assim, um sistema de cooperação jurídica em que os instrumentos tradicionais, notadamente o das cartas rogatórias, passaram a conviver com formas mais modernas, instituídas por fontes normativas de Direito Público Internacional. (ZAVASCKI, 2010, p.10).

Assim, a adoção por parte das nações de mecanismos que possibilitassem uma cooperação mútua mais desburocratizada surgiu da necessidade de criação de um sistema que permitisse que os órgãos de persecução penal estabelecessem comunicação eficiente, troca de informações, compartilhamento de provas e execução de medidas preventivas, investigatórias, instrutórias ou acautelatórias (ZAVASCKI, 2010, p. 12).

Apesar de ser evidente que um dos valores buscados pela cooperação internacional seja a eficiência da persecução penal, não se pode esquecer que essa busca não pode de forma alguma deixar de lado os direitos fundamentais dos cidadãos. Assim, deve-se abandonar aquela ideia inicial de que os acordos de cooperação deveriam ser vistos exclusivamente sobre um olhar bidimensional,

na medida em que visavam unicamente os interesses dos estados envolvidos. Atualmente, exige-se que esses acordos sejam vistos a partir de uma dimensão tridimensional em que, além dos interesses dos estados, devem ser tutelados os direitos fundamentais garantidos aos indivíduos (GRINOVER, 1995, p. 43-44).

Compartilhando sobre a mesma preocupação, Valente (2013, p. 87), ao analisar a cooperação judiciária europeia e internacional em matéria penal, pontua que a proteção efetiva dos direitos e liberdades fundamentais dos cidadãos constituem limites intransponíveis[2].

A reação dos estados para enfrentar esse novo fenômeno da criminalidade transnacional não parou apenas no aprimoramento da cooperação internacional para fins penais, evoluindo também no campo dos novos meios de investigação que se fizeram necessários para que as atividades de prevenção e instrução processuais fossem mais efetivas.

Assim, o avanço do crime organizado transnacional e do terrorismo também obrigou os estados a buscarem meios de obtenção de prova especializados que fossem capazes de proporcionar investigações mais eficientes, tais como interceptações telefônicas e ambientais, infiltrações policiais, videovigilância e rastreio digital (VALENTE, 2017, p. 474-475).

Além de todas essas medidas, é inegável que, com o avanço tecnológico, multiplicaram-se as possibilidades para uma investigação criminal, seja pelo fato de hoje em dia existir uma imensa quantidade de dados pessoais coletados nas atividades cotidianas das pessoas,

[2] Seguindo a mesma linha, Cervini (2013, p. 70), ao analisar o protocolo de assistência penal no âmbito do Mercosul, defende que o acordo sempre seja interpretado com a necessidade de integral respeito aos direitos fundamentais do homem.

seja pelo fato de que qualquer conduta delituosa acaba de alguma forma deixando uma pegada digital e isso abre possibilidade para a atuação dos órgãos de persecução (FERREIRA, 2021, p. 117-119).

Esse contexto exige que a tecnologia seja de fato empregada nas investigações criminais, especialmente através do legítimo tratamento de dados pessoais coletados dos indivíduos com a finalidade de prevenir ameaças geradas pela criminalidade organizada e pelo terrorismo (ARAS, 2020, p. 25).

Dessa forma, o uso de dados pessoais se mostra atualmente em crescente evolução, não apenas para auxiliar na colheita de provas no âmbito do processo penal, mas principalmente na utilização preventiva de todos esses dados para auxiliar na atuação dos órgãos de persecução penal. Esses dados muitas vezes são colhidos de forma massiva e processados por sistemas de inteligência artificial que buscam categorizar grupos e indivíduos com propensão à criminalidade. Entre esses novos usos, podem ser citados a polícia preditiva, as diversas tecnologias de vigilância e o processamento de dados com o objetivo de investigar crimes específicos (FERREIRA, 2021, p. 130).

A polícia preditiva se destaca entre esses usos objetivando prever áreas de criminalidade ou pessoas com alguma predisposição aos crimes a partir de dados históricos processados por algoritmos. Para auxiliar nesse processo são associadas diversas tecnologias, como o reconhecimento facial e o uso de drones e de sensores de ambiente (AZEVEDO; DUTRA, 2021, p. 254).

Por todo o exposto, verifica-se a evolução dos instrumentos de investigação e de cooperação entre os estados com a finalidade de enfrentar a nova realidade da criminalidade transnacional que se consolidou em um mundo globalizado.

Na sequência, será aprofundado o estudo sobre um desses novos instrumentos surgidos para auxiliar a persecução penal: o reconhecimento facial. Serão abordados conceitos gerais e aportes teóricos necessários para a compreensão desse novo mecanismo, incluindo a sua importância como uma eficiente ferramenta para a prevenção e para a investigação de crimes e, ainda, serão expostas as suas principais limitações no contexto mundial atual.

3 IDENTIFICAÇÃO BIOMÉTRICA E RECONHECIMENTO FACIAL: CONCEITOS E POSSIBILIDADES

A biometria pode ser conceituada como um mecanismo de reconhecimento das pessoas através dos traços morfológicos ou comportamentais (JAIN; PANKANTI, 2008, p. 78). Dentre os métodos que utilizam padrões morfológicos ou fisiológicos, podem ser citados, por exemplo, aqueles que usam impressões digitais, características da íris ou geometria da mão. Já os métodos que utilizam o comportamento humano abrangem, por exemplo, análise dos padrões da fala e a forma de assinatura do indivíduo[3] (MATA, 2020, p. 124).

Para o correto funcionamento de um sistema biométrico, exige-se que as características sejam individualizáveis em cada pessoa, além de ser necessário que os traços analisados não sofram mudanças significativas ao longo dos anos (JAIN; PANKANTI, 2008, p. 79).

Além disso, deve-se compreender que todos esses métodos não são infalíveis, sendo fundados predominantemente em análises

[3] Atualmente, existem diversas tecnologias voltadas à identificação biométrica, sendo que os principais métodos foram classificados pela Agência Brasileira de Desenvolvimento Industrial em três grupos: 1) sistemas de impressão digital; 2) sistemas de identificação de íris, DNA e face; e 3) sistemas de reconhecimento de voz (AGÊNCIA BRASILEIRA DE DESENVOLVIMENTO INDUSTRIAL, 2010, p. 61).

probabilísticas e, também, é necessário que sejam corretamente utilizados de acordo com a finalidade pretendida, não existindo um único método que seja adequado para todas as necessidades (JAIN; PANKANTI, 2008, p. 78-81).

Atualmente, os métodos de identificação biométrica são utilizados de forma automatizada, através de sistemas computacionais que capturam e codificam as características morfológicas ou comportamentais dos indivíduos (AGÊNCIA BRASILEIRA DE DESENVOLVIMENTO INDUSTRIAL, 2010, p. 60).

Uma das formas de identificação biométrica que vem sendo desenvolvida e utilizada atualmente é o reconhecimento facial. Essa modalidade, embora tenha se originado na década de 1960, passou por grande evolução após os atentados de 11 de setembro nos Estados Unidos (NUNES *et al*, 2016, p. 123).

Em termos gerais, essa técnica se utiliza da captação da imagem dos rostos dos indivíduos e, na sequência, um *software* auxiliado por algoritmos realiza o mapeamento matemático dessas imagens e os compara com padrões armazenados em bancos de dados (BIG BROTHER WATCH, 2018, p. 6). No mapeamento dos traços faciais de cada indivíduo, são considerados cerca de 80 pontos nodais, sendo que as relações existentes sobre esses pontos geram uma geometria espacial única, que é armazenada em forma de dados (MENA, 2018).

Em geral, os sistemas de reconhecimento facial seguem etapas durante o processo de reconhecimento. Inicialmente, ocorre a detecção do rosto, o qual é seguido pela extração e conversão em dados, para finalmente ocorrer a comparação com os bancos de dados existentes (KLARE *et al*, 2012, p. 3).

Essa tecnologia pode ser usada tanto para a verificação como para a identificação das pessoas. Os sistemas que objetivam a verificação basicamente comparam os dados capturados com os dados daquele mesmo indivíduo que estejam armazenados em um banco de dados. Os sistemas de identificação são um pouco mais elaborados, pois não partem de um indivíduo específico para comparar com os dados captados de uma face. Nesse sistema, são comparadas as informações extraídas do rosto de um indivíduo com informações de diversos indivíduos existentes em um banco de dados (AGÊNCIA BRASILEIRA DE DESENVOLVIMENTO INDUSTRIAL, 2010, p. 61).

Tanto a identificação como a verificação têm um grande potencial de auxílio na área da segurança pública, abarcando o policiamento preventivo, as investigações criminais e o combate ao terrorismo. A potencialidade desse novo instrumento tecnológico na persecução penal somente se desenvolveu graças à recente expansão das capacidades de coleta, armazenamento e processamento de dados, ao aumento dos dispositivos de captação de imagens e ao aprimoramento dos algoritmos de inteligência artificial[4] (BUOLAMWINI *et al*, 2020, p. 7).

Desta forma, verifica-se que o reconhecimento facial possui características que são valiosas para a atuação na segurança pública e na prevenção do terrorismo, especialmente pelos avanços tecnológicos que permitem uma enorme e constante captação de imagens com boa qualidade através de câmeras de vigilância espalhadas por todo o mundo. Além desse ambiente favorável à colheita de dados, também deve ser mencionado que essa forma de identificação biométrica permite que as autoridades públicas realizem um controle a distância

[4] Tanto a evolução da tecnologia de captação de imagens por máquinas digitais como a evolução da internet possibilitaram a formação de imensos bancos de dados de imagens que foram fundamentais para o treinamento dos algoritmos de reconhecimento facial e, consequentemente, para o desenvolvimento dessa tecnologia (LESLIE, 2020, p. 12).

sem que os indivíduos tenham ciência da realização do monitoramento (NUNES *et al*, 2016, p. 114).

Nesse ponto, o reconhecimento facial possui características positivas para a identificação biométrica, incluindo a universalidade, a aceitabilidade e, principalmente, a coletabilidade, pois não exige a cooperação do indivíduo para a obtenção dos dados[5] (UNIVERSIDADE DE BRASÍLIA, 2014, p. 44-46).

Expostos os contornos gerais do reconhecimento facial e a sua importância para a atividade persecutória, verificar-se-á nos próximos capítulos as limitações técnicas, práticas e jurídicas para a aplicação dessa tecnologia na persecução penal.

4 LIMITES TÉCNICOS AO USO DO RECONHECIMENTO FACIAL

Embora os programas de reconhecimento facial tenham evoluído muito nos últimos anos[6], estudos demonstram que essa tecnologia ainda comete muitas falhas quando utilizada em tempo real para identificar um indivíduo entre muitos.

Por exemplo, pesquisa realizada no País de Gales constatou um índice de 91% de correspondências equivocadas dentro de um total de 2.685 correspondências realizadas pelo sistema. A situação se mostrou

[5] Diferente, por exemplo, da utilização de impressão digital, que exige que a colheita se dê de forma física e com a anuência do indivíduo (AGÊNCIA BRASILEIRA DE DESENVOLVIMENTO INDUSTRIAL, 2010, p. 61).

[6] Nesse sentido, pode ser citado estudo elaborado pelo Instituto Nacional de Padrões e Tecnologia dos Estados Unidos – Nist, que realizou uma simulação para verificar a utilização do reconhecimento facial no controle de passageiros de 567 voos simulados, tendo obtido uma eficácia de 99,5% no reconhecimento facial positivo, em que se compara se uma determinada pessoa está presente em um banco de dados (GROTHER *et al*, 2021, p. 3-5).

ainda mais grave na atuação da Polícia Metropolitana do Reino Unido, na qual foi observado um índice de 98% de correspondências erradas (BIG BROTHER WATCH, 2018, p. 29).

Esses números são muito preocupantes se pensarmos que na área da segurança pública e da prevenção do terrorismo se necessita exatamente que os sistemas de reconhecimento facial sejam programados para identificar um indivíduo entre muitos em tempo real.

Ao se analisar um panorama geral sobre os estudos relacionados aos programas de reconhecimento facial, verifica-se que as principais causas de erros do sistema decorrem da má qualidade da imagem captada, estando normalmente relacionadas à iluminação da imagem, ao ângulo obtido ou a eventuais expressões contidas na face[7] (KLARE *et al*, 2012, p. 1).

Em geral, os sistemas de reconhecimento facial são extremamente precisos quando utilizados em condições favoráveis. Assim, quando a captação da imagem é frontal, com uma boa iluminação e com a expressão da face neutra, a acurácia dos sistemas é maior, o que não ocorre quando a imagem da face é captada com alterações na pose, na iluminação ou quando a pessoa está utilizando acessórios faciais ou tem barba (JAIN; PANKANTI, 2008, p. 80).

Embora venham sendo desenvolvidos programas voltados a aprimorar a detecção e o reconhecimento das faces e, consequentemente, que possam superar todas essas dificuldades (SATO *et al*, 2005, p. 28-31), as limitações no uso dessa tecnologia ainda são relevantes. Nesse sentido, estudo capitaneado por Klontz e

[7] Por exemplo, se a imagem captada tiver um sorriso ou estiver com os olhos fechados, isso gerará dificuldades na atuação dos sistemas de reconhecimento facial (MATA, 2020, p. 131).

Jain (2013, p. 91-94) analisou fotografias de suspeitos do atentado de Boston ocorrido em 2013 e verificou que a baixa qualidade das fotos extraídas de filmagens e a existência de óculos na face dos suspeitos dificultam a eficácia do processo de identificação.

Outro ponto que gera inúmeras dificuldades ao funcionamento dos programas de reconhecimento facial diz respeito às decisões enviesadas geradas pela programação dos algoritmos.

Os sistemas de reconhecimento facial automatizados se utilizam de algoritmos para o seu correto funcionamento. E são usados algoritmos inteligentes capazes de criar algoritmos e, consequentemente, escrever seus próprios programas – o que se convencionou denominar como *machine learning* (MENDES; MATTIUZZO, 2019, p. 44). Em outras palavras, a técnica de *machine learning* utiliza algoritmos para coletar e interpretar dados. Mas para que isso funcione, é necessário que processe um grande volume de dados que permitam o aprendizado do algoritmo (FERRARI; BECKER; WOLKART, 2018, p. 639).

Embora os algoritmos partam de uma importante premissa de buscar decisões mais objetivas que fujam do subjetivismo e da arbitrariedade (QUATTROCOLO, 2019, p. 1528), nem sempre isso acontece, seja por falhas na própria programação ou mesmo no treinamento dos algoritmos (MENDES; MATTIUZZO, 2019, p. 51-54).

No âmbito do reconhecimento facial, estudos verificaram que, em muitas ocasiões, os sistemas foram programados a partir de pressupostos técnicos que privilegiavam a pele clara, como ocorreu na evolução da tecnologia das fotografias (LESLIE, 2020, p. 6, 14). Assim, a falha na própria programação dos algoritmos é capaz de gerar erros no sistema de reconhecimento facial, especialmente aqueles relacionados

ao reconhecimento de pessoas negras[8] e de mulheres (BUOLAMWINI; GEBRU, 2018, p. 11).

Nesse sentido, uma pesquisa liderada por Buolamwini e Gebru (2018, p. 11) analisou diversos algoritmos de reconhecimento facial e constatou que a precisão dos sistemas são piores em relação às mulheres e aos negros. Os números são preocupantes e revelam, por exemplo, uma diferença de até 20,6% de erros no reconhecimento de mulheres em relação aos homens e de até 19,2% de erros no reconhecimento de pessoas negras em relação a pessoas brancas.

Além de falhas na programação dos algoritmos, muitas vezes os vieses verificados nos sistemas decorrem de falhas nos treinamentos dos algoritmos. Assim, o aprimoramento dos sistemas de reconhecimento facial depende de efetivo treinamento que se dá através do processamento de milhões de imagens de rostos (GATES, 2014, p. 12). Ocorre que, no treinamento dos programas de reconhecimento facial, muitas vezes são usados bancos de dados que representam de forma preponderante grupos sociais e raciais dominantes, deixando uma menor participação para grupos marginalizados, o que gera, por consequência, uma piora na qualidade do sistema (LESLIE, 2020, p. 13-17).

Para comprovar esse fator de ineficiência dos sistemas, foi realizada pesquisa pelo Instituto Nacional de Padrões e Tecnologia dos Estados Unidos – Nist, que verificou a maior ocorrência de erros do sistema em relação a negros, asiáticos, mulheres, crianças e idosos. Entre as conclusões da pesquisa, chama a atenção a

[8] Caso que se tornou rumoroso nos Estados Unidos ocorreu após a prisão de Robert Julian Borchak Williams em Detroit, em janeiro de 2020. A prisão de Williams, que é negro, decorreu de um alerta equivocado do sistema de reconhecimento facial da polícia (ANDERSON, 2020). No Brasil, também foi verificado problema similar com uma prisão sendo realizada em razão de falha no sistema de reconhecimento facial conforme noticiado pela imprensa (WERNECK, 2019).

constatação de que a localização do desenvolvedor do algoritmo e a consequente alimentação dos dados demográficos influenciavam de forma significativa o desempenho do programa (GROTHER; NGAN; HANAOKA, 2019, p. 10).

Por todo o exposto, verifica-se que, embora tenha ocorrido uma grande evolução nos programas de reconhecimento facial automatizado, ainda existem relevantes limites técnicos que, muitas vezes, podem ocasionar identificações erradas e causar sérios prejuízos aos indivíduos.

5 LIMITES PRÁTICOS RELACIONADOS À UTILIZAÇÃO DO RECONHECIMENTO FACIAL

Para que os sistemas de reconhecimento facial tenham efetividade na utilização na área da segurança pública ou mesmo na prevenção da criminalidade organizada transnacional ou do terrorismo, é necessário que existam bancos de dados completos e integrados entre os órgãos de inteligência e de persecução penal dos diversos países.

Num primeiro ponto, para que os sistemas sejam efetivos, exige-se que os bancos de dados sejam completos e contenham os padrões faciais do maior número de pessoas possível. Sem esse banco de dados completo fica prejudicada a lógica do sistema, pois não existirão padrões para a realização das comparações "de um para muitos". Uma amostra dessa necessidade pode ser constatada pela análise do atentado de 11 de setembro de 2001 no qual, na época, apenas dois terroristas eram conhecidos do sistema de segurança norte-americano, sendo que apenas um deles possuía foto no sistema (NUNES *et al*, 2016, p. 124).

Além da existência de bancos de dados completos, para que o sistema de reconhecimento facial automatizado seja efetivo na prevenção delitiva e na instrução criminal é necessário que esses bancos de dados sejam integrados entre as diversas forças de segurança das nações. Sem esse real compartilhamento de informações, a aplicabilidade da tecnologia ficaria restrita à criminalidade local. E, como foi visto nos capítulos anteriores, atualmente a criminalidade organizada e o terrorismo deixaram de atuar de forma local e passaram a atuar de forma integrada por todo o mundo.

Essa criminalidade supranacional atua sem fronteiras e em escala mundial, o que exige que os estados criem instrumentos jurídicos que sejam aptos a efetivar um combate que também não seja restringido por fronteiras físicas (LESSA, 2016, p. 117).

Assim, mostra-se fundamental que acordos sejam firmados entre os países e que as legislações nacionais sigam *standards* mínimos de proteção dos direitos individuais.

Nesse aspecto, o reconhecimento facial, por se utilizar de dados biométricos sensíveis dos indivíduos, deve ter a sua implementação pautada pela atuação do Estado de acordo com a lei e com a proteção dos direitos fundamentais asseguradas por tratados internacionais e pelas constituições nacionais.

Sobre a importância da aplicação das leis de proteção de dados pessoais também à atuação de persecução penal, são importantes as explicações de Aras:

> Nesse sentido, as normas de proteção de dados pessoais devem aplicar-se também ao Estado quando coleta, manipula e difunde dados

> pessoais de investigados, suspeitos, réus, vítimas, testemunhas, peritos, autoridades e funcionários que atuam na persecução criminal e de terceiros eventualmente alcançados por medidas de apuração. Investigações criminais e medidas de segurança pública são atividades estatais que interferem rotineiramente na vida dos cidadãos, tornando-se relevante a perspectiva da privacidade. Por outro lado, é preciso regular adequadamente a transferência internacional de dados para atividades empresariais e para a cooperação internacional nos campos policial e judicial, temática essencial num mundo hiperconectado. Como em tudo na vida, a virtude está no plano médio. Tais proteções não devem inviabilizar os métodos operacionais do Estado na elucidação de crimes. Cada vez mais dependemos de meios tecnológicos de investigação para a descoberta de crimes, especialmente para a determinação de autoria. (ARAS, 2020, p. 25).

Assim, é importante que os países tenham legislações modernas que prevejam todas essas proteções aos indivíduos e que, ao mesmo tempo, garantam a segurança jurídica aos operadores do sistema. Nesse ponto, a existência de legislações nacionais que respeitem os *standards* mínimos previstos em tratados internacionais se mostra fundamental para permitir uma efetiva e segura integração entre os órgãos de persecução dos diversos países.

6 LIMITAÇÕES JURÍDICAS: O RECONHECIMENTO FACIAL VIOLA DIREITOS FUNDAMENTAIS?

Como foi visto ao longo do texto, a utilização de sistemas de reconhecimento facial se relaciona com a extração de dados biométricos dos indivíduos, atuando, portanto, com a coleta de

informações sensíveis dos cidadãos[9]. No caso do reconhecimento facial, a preocupação com a proteção de dados é ainda maior pelo fato de essa extração de informações se dar sem a ciência e sem o consentimento do indivíduo.

Dessa forma, uma primeira preocupação existente se relaciona com a proteção de dados pessoais[10]. Embora no Brasil ainda não exista uma legislação específica que trate da proteção de dados pessoais para a utilização na segurança pública e na instrução criminal, os princípios gerais da Lei Geral de Proteção de Dados (BRASIL, 2018) devem ser invocados sempre que se trate da coleta de dados sensíveis, como é o caso da tecnologia do reconhecimento facial. Assim, qualquer projeto que opte por utilizar essa tecnologia no Brasil deve respeitar os princípios da adequação, da necessidade, da qualidade dos dados, da segurança, da prevenção de danos e da não discriminação (MALDONADO; BLUM, 2020, p. 75).

Para uma melhor compreensão da importância do assunto, é importante perceber que a proteção de dados dos indivíduos está intimamente relacionada aos direitos da personalidade. Nesse sentido, Mendes (2020, p. 1-15) traça a evolução dos julgamentos proferidos pelo Tribunal Constitucional Alemão, que culminou com a decisão sobre o censo ocorrida em 1983. De acordo com a autora, naquela época, o tribunal alemão considerou que as inovações tecnológicas no processamento dos dados pessoais exigem uma evolução na interpretação dos direitos fundamentais. Assim, com base na proteção

[9] Cabe referir que nem todo processamento de imagens envolve o de dados sensíveis, o que apenas ocorre naqueles casos em que o processamento se dá por um meio técnico que permita a identificação ou a autenticação individualizada de uma pessoa (CONSELHO DA EUROPA, 2021, p. 3).

[10] Em data recente, a Emenda Constitucional n. 115, de 2022, incluiu expressamente no art. 5º, LXXIX, a proteção de dados pessoais como um direito fundamental nos seguintes termos: "É assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais". (BRASIL, 2022).

da personalidade dos indivíduos, a corte alemã verificou que não bastava mais uma proteção sobre a natureza das informações que seriam coletadas das pessoas, mas agora interessava também a forma como essas informações seriam processadas e os riscos que aquele processamento traria para os direitos da personalidade. Daí, surge o direito à autodeterminação informativa que influenciou tantos ordenamentos estrangeiros e que, inclusive, está incorporado na Lei Geral de Proteção de Dados brasileira.

Verifica-se uma evolução sobre a proteção da privacidade que inicialmente se resumia a uma dimensão negativa, na qual terceiros não poderiam invadir espaços privados, e atualmente possui uma dimensão positiva que abrange a necessária atuação positiva que proteja também a maneira como os dados vão circular de forma que o indivíduo não perca o controle sobre as suas próprias informações (MORAES; QUEIROZ, 2019, p. 118).

Dessa forma, observa-se que os danos que podem ser causados com o acesso aos dados pessoais não se resumem à sua coleta, mas também podem gerar sérias consequências após o seu processamento – como o que ocorre com empresas privadas, que se utilizam dos dados para pautarem suas ações de *marketing*[11], ou mesmo pelas forças de segurança que podem utilizar da coleta massiva de dados para detectar crimes e suspeitos (FROOMKIN, 2000, p. 1469-1471).

Essa coleta massiva de dados pode se dar através de diversos mecanismos, como a utilização de câmeras de vigilância, a localização de telefones celulares, veículos e de aplicativos, o reconhecimento de voz, entre outros (FROOMKIN, 2000, p. 1475-1481), sendo a utilização

[11] Sobre o capitalismo de vigilância e a força dessas empresas na atualidade cabe a leitura da obra de Zuboff (2020).

do reconhecimento facial automatizado um desses mecanismos que possibilitam a coleta massiva de dados pessoais – o que permite que o Estado tenha ciência de cada passo dado por seus cidadãos[12].

Dentro desse contexto, o reconhecimento facial sofre críticas por ser um dos instrumentos que auxiliam na implementação de sistemas de vigilância massiva das pessoas. Sobre a vigilância em massa, Milaj e Bonnici (2014, p. 419-423) argumentam que, atualmente, dever-se-ia falar em uma sociedade pré-crime, e não em uma sociedade pós-crime, pois as pessoas são previamente investigadas mesmo que não tenham nenhuma relação com atividades delituosas. Partindo dessa visão, os autores defendem que programas de vigilância em massa violariam o princípio da presunção da inocência. Essa conclusão decorre de uma interpretação mais ampla desse princípio, o que abrange a proteção contra qualquer ato que possa gerar uma investigação contra uma pessoa.

Dessa realidade de vigilância de massa, extrai-se uma relevante preocupação com a invasão das esferas individuais das pessoas que, ao terem ciência de que seus passos estão cada vez mais monitorados pelo Estado, acabam deixando de fazer ou de ser o que gostariam. É o que a doutrina denomina como *chilling effect* e que nada mais é do que uma consequência de uma sociedade fundada em uma cultura de suspeita em que prepondera o medo e a desconfiança (MILAJ; BONNICI, 2014, p. 420).

Nesse ponto, a utilização do reconhecimento facial pode ser danosa para o desenvolvimento da personalidade das pessoas, incluindo o direito de expressão. Por exemplo, quando utilizado em

[12] Nesse sentido, observa-se que, em alguns países, o sistema de controle que utiliza o reconhecimento facial como uma das suas ferramentas chegou ao ponto de possibilitar o controle das pessoas por *scores* (ZYLBERMAN, 2020).

espaços públicos, pode inibir um protesto, limitando consequentemente a participação cívica e democrática dos cidadãos (LEMOS *et al*, 2021, p. 5).

Cabe referir, ainda, que a preocupação com a privacidade e com a autodeterminação informativa não se restringe à esfera de cada indivíduo, mas sim de toda a sociedade que pressupõe a liberdade para que todos façam as suas escolhas (FERREIRA, 2021, p. 134).

No que toca ao reconhecimento facial, todas essas preocupações são extremamente pertinentes, pois a utilização dessa ferramenta possui o potencial de colocar em risco direitos fundamentais dos cidadãos, incluindo a privacidade, as liberdades de expressão e a associação e a presunção de inocência (LEMOS *et al*, 2021, p. 1).

Por todos esses motivos, é relevante que o tema seja devidamente discutido pela sociedade e que se busquem soluções que permitam o aproveitamento das novas tecnologias sem qualquer violação de direitos fundamentais.

7 PERSPECTIVAS E CAMINHOS PARA O USO EFICIENTE DO RECONHECIMENTO FACIAL

Os sistemas de reconhecimento facial automatizados são aplicados em grande parte dos países[13], especialmente nas áreas de segurança pública e privada, movimentando atualmente um montante aproximado de 3,8 bilhões de dólares (FACIAL..., 2020).

No Brasil, verifica-se a utilização da tecnologia, especialmente na área do transporte e da segurança pública (INSTITUTO IGARAPÉ, c2022), observando-se que até 2019 se averigua pelo menos 13 projetos de sistemas de reconhecimento facial voltados à segurança pública (FRANCISCO; HUREL; RIELLI, 2020, p. 2).

Essas primeiras iniciativas foram se expandindo, sendo a tecnologia incluída como uma das medidas adotadas pelo Ministério da Justiça e Segurança Pública para o combate da criminalidade violenta[14], além de dar apoio a novos sistemas de identificação utilizados pela Polícia Federal brasileira[15].

Embora essa nova tecnologia venha sendo utilizada no Brasil e no mundo, existem inúmeras resistências a sua expansão, especialmente com as preocupações, elencadas ao longo do texto, com a proteção dos direitos fundamentais, incluindo a privacidade, as diversas liberdades e os dados sensíveis. Também existem preocupações com a vigilância em

[13] Mapa demonstra que a tecnologia está sendo aplicada em grande parte dos países do globo (THE FACIAL..., 2020).

[14] Nesse sentido, o art. 4º, § 1º, III, *b*, da Portaria n. 793/2019 dispõe sobre o "fomento à implantação de sistemas de videomonitoramento com soluções de reconhecimento facial, por Optical Character Recognition – OCR, uso de inteligência artificial ou outros" (BRASIL, 2019b).

[15] Atualmente, a Polícia Federal brasileira implementou um sistema de identificação biométrica denominado Solução Automatizada de Identificação Biométrica – Abis, que abrange tanto a impressão digital como o reconhecimento facial (BRASIL, 2021).

massa e seus nefastos efeitos em uma sociedade e, também, com o alto índice de erros dos sistemas de reconhecimento facial, principalmente aqueles que atingem classes historicamente marginalizadas.

Esse movimento contrário ao uso da tecnologia fez com que o reconhecimento facial automatizado fosse proibido em um aeroporto da Bélgica (BELGIAN..., 2019) e em alguns estados norte-americanos (FRANCISCO; HUREL; RIELLI, 2020, p. 9-10). No âmbito judicial, a Corte de Apelação de Cardiff, no País de Gales, decidiu que a polícia local violou direitos humanos ao utilizar os sistemas de reconhecimento facial em desacordo com a lei (ROYAL COURTS OF JUSTICE, 2020).

Por outro lado, existe forte apoio pela utilização da tecnologia, especialmente por se mostrar uma relevante ferramenta de combate e prevenção ao crime organizado e ao terrorismo internacional[16].

Nesse sentido, importante decisão da Corte Europeia de Direitos Humanos, no caso Big Brother Watch e outros *vs.* Reino Unido, tratou do tema da vigilância em massa. Embora não tenha se referido expressamente à tecnologia do reconhecimento facial, a corte europeia declarou, por maioria, que programas de vigilância em massa são admissíveis desde que respeitem a regulamentação e a imposição de salvaguarda pelos países (EUROPEAN COURT OF HUMAN RIGHTS, 2021)[17], inclusive superando a posição em sentido diverso da corte no caso Szábo e Viss *vs* Hungria (EUROPEAN COURT OF HUMAN RIGHTS, 2016)[18].

[16] Não se pode esquecer que esse apoio é fortalecido pelas grandes empresas de tecnologia, que são as principais desenvolvedoras e fornecedoras dos programas de reconhecimento facial.

[17] O caso se originou de três diferentes pedidos que decorreram das revelações feitas por Edward Snowden sobre programas de vigilância eletrônica realizados pelos serviços de informações dos Estados Unidos e do Reino Unido.

[18] Caso em que a Corte Europeia censurou a prática de interceptações genéricas em uma área em que ocorra um crime.

Fixadas essas premissas, que de alguma forma resumem o atual estado do debate mundial sobre o uso do reconhecimento facial na área da segurança pública, a partir desse momento se buscará expor os principais pontos levantados ao longo do texto para que, na sequência, se possa posicionar sobre esse tema tão relevante.

De início, deve-se pontuar que a tecnologia do reconhecimento facial se desenvolveu muito nos últimos anos, sendo uma ferramenta imprescindível para a utilização em investigações relacionadas ao crime organizado transnacional e ao terrorismo. O atual ambiente em que vivemos, com imenso monitoramento por vídeo, permite que o reconhecimento facial seja extremamente eficiente na localização e identificação instantânea de criminosos e terroristas, o que pode ser muito útil tanto na prevenção de crimes como na investigação desses delitos.

Essa possibilidade quase instantânea de localizar suspeitos e criminosos em tempo real, sem que tenham ciência, é uma ferramenta inigualável em termos de eficiência e permite que a tecnologia seja utilizada em conjunto com outros meios de investigação para o enfrentamento dessas organizações criminosas que estão cada vez mais profissionalizadas.

Ocorre que a tecnologia do reconhecimento facial ainda necessita de diversos aprimoramentos técnicos para evitar a ocorrência de falsos negativos, que atrapalham as investigações e, principalmente, de falsos positivos, que podem causar danos irreversíveis para os cidadãos que sejam incorretamente identificados.

Além disso, os programas devem evoluir para que não ocorram vieses raciais e de gênero que, como foi visto ao longo do trabalho,

aumentam demasiadamente a possibilidade de identificações erradas em relação a mulheres e pessoas da raça negra.

Nesse sentido, cabe mencionar as recomendações constantes na Convenção 108 do Conselho da Europa (CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA, 2021), que traz diversas diretrizes voltadas ao aprimoramento do reconhecimento facial. Entre essas diretrizes, que são voltadas aos legisladores, desenvolvedores e aplicadores da tecnologia, estão aquelas em que se busca um aprimoramento técnico da tecnologia.

Embora a correção desses defeitos técnicos dos sistemas de reconhecimento facial seja urgente, para que tal ferramenta seja efetiva no combate ao crime transnacional também é necessário que haja uma aproximação entre os países de forma que bancos de dados possam ser compartilhados e, com isso, possam de fato ser aptos a auxiliar em investigações internacionais.

Por outro lado, o reconhecimento facial gera uma série de preocupações relacionadas à proteção de dados sensíveis e à violação de direitos fundamentais dos indivíduos. Para evitar e minorar qualquer violação de direitos, é muito importante que a utilização desse meio tecnológico se dê de forma cautelosa e seja pautada por limitações legais ou regulamentares que estabeleçam diretrizes e limitações ao uso da tecnologia e, também, que coíbam eventuais excessos por parte dos órgãos de persecução penal.

Por exemplo, no Reino Unido, a regulamentação se dá através da utilização de vários documentos recomendatórios, enquanto na França, além de uma lei específica, exige-se autorização dos

órgãos competentes após prévio estudo sobre os possíveis impactos (FRANCISCO; HUREL; RIELLI, 2020, p. 6-12).

No Brasil, ainda não existe uma lei geral que trate sobre o reconhecimento facial[19], assim como não existe uma lei que trate da proteção pessoal de dados para fins específicos de uso na segurança pública, o que gera um vácuo legislativo que, por um lado, cria um ambiente de insegurança jurídica para os investigadores e, também, deixa um perigoso espaço para a ocorrência de violações de direitos fundamentais dos indivíduos.

Talvez a vigência de uma lei de proteção de dados para a segurança pública possa definir um caminho mais seguro na regulamentação desse tipo de tecnologia. Nesse sentido, em 2020 foi apresentado um anteprojeto de lei dispondo sobre uma lei geral de proteção de dados para a segurança pública e a persecução penal (BRASIL, 2019a). O referido anteprojeto de lei, embora não tenha se referido expressamente sobre as tecnologias de reconhecimento facial, tratou genericamente das tecnologias de monitoramento elencando pelo menos dois requisitos necessários para a sua implementação: autorização legal prévia e específica (art. 42); e que haja conexão com uma investigação específica autorizada por lei e por decisão judicial (art. 43) (LEMOS *et al*, 2021, p. 4).

Além da importância de uma legislação específica sobre o reconhecimento facial em um contexto de criminalidade organizada transnacional e de grupos terroristas internacionais, mostra-se relevante que existam caminhos de comunicação e troca de informação entre os diversos países. Esses caminhos normalmente se materializam mediante tratados internacionais e de acordos bilaterais entre as nações.

[19] O Distrito Federal foi a primeira unidade da Federação a dispor sobre uma legislação específica a respeito do reconhecimento facial (DISTRITO FEDERAL, 2020).

Também nesse aspecto, o Brasil está atrasado em relação aos demais países, pois ainda não possui uma legislação de proteção de dados específica para a segurança pública nos moldes da Diretiva n. 680/2016 (UNIÃO EUROPEIA, 2016), que está em vigor na Europa. Nesse sentido, Aras (2020, p. 26-29) defende que o Brasil busque uma simetria com a legislação europeia para que não fiquem prejudicadas as cooperações internacionais a serem realizadas pelo Brasil. Refere ainda o autor que a falta dessa legislação vem prejudicando o compartilhamento de dados referentes a cidadãos residentes na União Europeia.

Assim, exige-se a criação de uma lei que trate sobre a proteção e a transferência de dados pessoais em matéria penal, sendo essa exigência fundamental para que sejam resguardados os direitos fundamentais dos indivíduos e, também, para que o Estado possa cumprir o seu papel de prevenção e repressão delitiva[20] (VIOLA; HERINGER; CARVALHO, 2021, p. 5).

Para tentar suprir essa carência, o projeto da Lei Geral de Proteção de Dados para a segurança pública e a persecução penal prevê disciplina similar àquela prevista pela Diretiva n. 680/2016, a qual permite a troca de dados entre os países por três vias: primeiramente, com base em uma decisão de adequação; não sendo possível a primeira

[20] Nesse sentido, deve ser citado o teor de parte da exposição de motivos do anteprojeto da Lei Geral de Proteção de Dados na esfera da segurança pública que bem sintetiza essa ideia: "Nesse contexto, a elaboração de uma legislação específica fundamenta-se na necessidade prática de que os órgãos responsáveis por atividades de segurança pública e de investigação/repressão criminais detenham segurança jurídica para exercer suas funções com maior eficiência e eficácia – como pela participação em mecanismos de cooperação internacional –, porém sempre de forma compatível com as garantias processuais e os direitos fundamentais dos titulares de dados envolvidos. Trata-se, portanto, de projeto que oferece balizas e parâmetros para operações de tratamento de dados pessoais no âmbito de atividades de segurança pública e de persecução criminal, equilibrando tanto a proteção do titular contra mau uso e abusos como acesso de autoridades a todo potencial de ferramentas e plataformas modernas para segurança pública e investigações." (BRASIL, 2019a).

via, a transferência pode se dar por meio da exigência de garantias adequadas de proteção de dados; e, subsidiariamente, admite-se uma terceira via em que as transferências de dados ocorram por meio de acordos firmados diretamente pelos países (VIOLA; HERINGER; CARVALHO, 2021, p. 7-9).

A integração entre os países também no nível legislativo com a fixação de *standards* mínimos de proteção de dados é muito importante para permitir uma eficiente cooperação, além de garantir que os direitos fundamentais sejam respeitados com a efetiva proteção dos dados pessoais.

8 CONCLUSÃO

O uso da tecnologia vem permitindo um considerável progresso nas estratégias de investigação adotadas por diversos países, especialmente para o enfrentamento de uma criminalidade internacional que cada vez mais está profissionalizada.

Dentro dessa realidade, a utilização dos sistemas de reconhecimento facial automatizados possui um grande potencial na busca por uma investigação mais eficiente que seja capaz de prevenir e de coibir práticas delitivas tão sofisticadas.

Ocorre que a busca pela eficiência a qualquer custo não pode ser justificativa para o uso descontrolado dessa ferramenta investigativa. Existem limites que devem ser respeitados sob pena de frontal violação de direitos fundamentais dos cidadãos.

Partindo dessa ideia, essa ferramenta deve ser utilizada com cautela, pois, como foi relatado ao longo do estudo, ainda possui

limitações técnicas que podem levar a identificações incorretas e consequentemente trazer prejuízos concretos para os indivíduos.

Além dos possíveis erros, o reconhecimento facial não pode ser utilizado sem limites, o que colocaria em risco os direitos fundamentais das pessoas e abriria caminho para a concretização de abusos por parte das agências de investigação.

Para evitar esses danos, o trabalho sugeriu que a tecnologia do reconhecimento facial e a transferência de dados entre os países devam ser devidamente regulados com o objetivo de trazer segurança jurídica tanto para os operadores dos sistemas como para os cidadãos que terão seus direitos protegidos.

REFERÊNCIAS

AGÊNCIA BRASILEIRA DE DESENVOLVIMENTO INDUSTRIAL. **Sistemas aplicados à segurança pública**. Brasília, DF: ABDI, jun. 2010. (Cadernos Temáticos, Tecnologias de Informação e Comunicação, 3). Disponível em: https://livroaberto.ibict.br/bitstream/1/536/1/Caderno%20Tem%c3%a1tico%20TIC%20-%203%20%28Vers%c3%a3o%20Final%29-%20Sistemas%20Aplicados%20a%20Seguran%c3%a7a%20Publica.pdf. Acesso em: 12 mar. 2022.

ALVES, Paulo Magno de Melo Rodrigues. O impacto de Big Data na atividade de inteligência. **Revista Brasileira de Inteligência**, Brasília, DF, n. 13, p. 1-20, dez. 2018.

ANDERSON, Elisha. Controversial detroit facial recognition got him arrested for a crime he didn´t commit. **Detroit Free Press**, Detroit, 11 July 2020. Disponível em: https://www.freep.com/story/news/local/michigan/detroit/2020/07/10/facial-recognition-detroit-michael-oliver-robert-williams/5392166002/. Acesso em: 3 mar. 2022.

ANDREATO, Danilo. Criminalidade transnacional, persecução penal global. *In:* BRASIL. Ministério Público Federal. Secretaria de Cooperação Internacional. **Temas de cooperação internacional**. 2. ed., rev. e atual. Brasília, DF: MPF, 2016. (Coleção MPF Internacional, 2). p. 147-154. Disponível em: https://memorial.mpf.mp.br/es/vitrine-virtual/publicacoes/temas-de-cooperacao-internacional-2a-edicao-revista-e-ampliada. Acesso em: 2 mar. 2022.

ARAS, Vladmir. A título de introdução: segurança pública e investigações criminais na era da proteção de dados. *In*: ASSOCIAÇÃO NACIONAL DOS PROCURADORES DA REPÚBLICA; BRASIL. Ministério Público Federal. 3. Câmara de Coordenação e Revisão. **Proteção de dados pessoais e investigação criminal**. Brasília, DF: ANPR, 2020. p. 14-31.

AZEVEDO, Rodrigo Ghiringhelli de; DUTRA, Luíza Correa de Magalhães. Inteligência artificial, big data e algoritmos: policiamento e as novas roupagens de um agir discriminatório. **Revista Brasileira de Ciências Criminais**, São Paulo, v. 29, n. 183, p. 247-268, set. 2021.

BELGIAN police stop facial recognition at Zaventem airoport. **Tellerreport**, [*s. l.*], Sept. 2019.

BIG BROTHER WATCH. **Face off**: the lawless growth of facial recognition in UK policing. [*S. l.*]: BBW, May 2018. Disponível em: https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf. Acesso em: 10 mar. 2022.

BRASIL. Câmara dos Deputados. **Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal**. Brasília, DF: Câmara dos Deputados, 2019a. Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/documentos/outros-documentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf. Acesso em: 12 mar. 2022.

BRASIL. Congresso Nacional. **Emenda Constitucional n. 115, de 10 de fevereiro de 2022**. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília, DF: Presidência da República, 2022. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 18 maio 2022.

BRASIL. Congresso Nacional. **Lei n. 13.709, de 18 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: https://legislacao.presidencia.gov.br/atos/?tipo=LEI&numero=13709&ano=2018&ato=293QzZ61UeZpWT79e. Acesso em: 11 mar. 2022.

BRASIL. Ministério da Justiça e Segurança Pública. Comunicação Social da Polícia Federal. **Polícia Federal implementa nova solução automatizada de identificação biométrica**. Brasília, DF: Ministério da Justiça e Segurança Pública, 6 jul. 2021. Disponível em: https://www.gov.br/pf/pt-br/assuntos/noticias/2021/07/policia-federal-implementa-nova-solucao-automatizada-de-identificacao-biometrica. Acesso em: 11 mar. 2022.

BRASIL. Ministério da Justiça e Segurança Pública. Portaria n. 793, de 24 de outubro de 2019. 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 [...]. **Diário Oficial da União**: seção 1, Brasília, DF, n. 208, p. 55, 25 out. 2019b. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-793-de-24-de-outubro-de-2019-223853575. Acesso em: 11 mar. 2022.

BUOLAMWINI, Joy *et al*. **Facial recognition technologies**: a primer. [*S. l.*]: Algorithmic Justice League: MacArthur Foundation, 29 May 2020. Disponível em: https://global-uploads.webflow.com/5e027ca188c99e3515b404b7/5ed1002058516c11edc66a14_FRTsPrimerMay2020.pdf. Acesso em: 5 mar. 2022.

BUOLAMWINI, Joy; GEBRU, Timnit. Gender shades: intersectional accuracy disparities in commercial gender classification. *In*: CONFERENCE ON FAIRNESS, ACCOUNTABILITY, AND TRANSPARENCY, 2018, New York City. **Proceedings** [...]. New York City: FAT, 2018. p. 1-15. Disponível em: https://dam-prod.media.mit.edu/x/2018/02/06/Gender%20Shades%20Intersectional%20Accuracy%20Disparities.pdf. Acesso em: 5 mar. 2022.

CERVINI, Raúl. La confidencialidad de las medidas cautelares em la cooperación judicial penal internacional: su relación com el ejercicio efectivo de la magistratura de la defensa, em particular, a la luz del protocolo del Mercosur. **Sistema Penal & Violência**, Porto Alegre, v. 5, n. 1, p. 60-72, jan./jun. 2013.

CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA, 108., 2021, [*s. l.*]. **Guidelines on Facial Recognition**. [Europa]: Council of Europe, 2021. Disponível em: https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3. Acesso em: 12 mar. 2022.

DISTRITO FEDERAL. Lei n. 6.712, de 10 de novembro de 2020. Dispõe sobre o uso de tecnologia de reconhecimento facial – TRF na segurança pública e dá outras providências. **Diário Oficial do Distrito**

Federal: Brasília, DF, ano 49, n. 213, 11 nov. 2020. Disponível em: https://www.tjdft.jus.br/institucional/relacoes-institucionais/arquivos/lei-no-6-712-de-10-de-novembro-de-2020.pdf. Acesso em: 12 mar. 2022.

EUROPEAN COURT OF HUMAN RIGHTS. Fourth Section. **Case of Szabó and Vissy vs Hungary**: (Application no. 37138/14). Strasbourg: ECHR, 12 Jan. 2016. Disponível em: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-160020%22]}. Acesso em: 11 mar. 2022.

EUROPEAN COURT OF HUMAN RIGHTS. Grand Chamber. **Case of Big Brother Watch and others vs The United Kingdom**: (Applications nos. 58170/13, 62322/14 and 24960/15). Strasbourg: ECHR, 25 May 2021. Disponível em: https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22case%20big%20brother%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-210077%22]}. Acesso em: 11 mar. 2022.

FACIAL recognition market worth $8,5 billion by 2025. [*S. l.*]: MarketsandMarkets, Dec. 2020. Disponível em: https://www.marketsandmarkets.com/PressReleases/facial-recognition.asp. Acesso em: 10 mar. 2022.

FERRARI, Isabela; BECKER, Daniel; WOLKART, Erik Navarro. "Arbitrium ex machina": panorama, riscos e a necessidade de regulação das decisões informadas por algoritmos. **Revista dos Tribunais**, São Paulo, v. 107, n. 995, p. 635-655, set. 2018.

FERREIRA, André da Rocha. Tratamento de dados pessoais em investigações criminais: o direito fundamental à autodeterminação informativa como limite constitucional. **Revista Brasileira de Ciências Criminais**, São Paulo, v. 29, n. 185, p. 115-159, nov. 2021.

FRANCISCO, Pedro Augusto P.; HUREL, Louise Marie; RIELLI, Mariana Marques. **Regulação do reconhecimento facial no setor público**: avaliação de experiências internacionais. Rio de Janeiro: Instituto Igarapé; [São Paulo]: Data Privacy Brasil Research, jun. 2020. Disponível em: https://igarape.org.br/wp-content/uploads/2020/06/2020-06-09-Regula%C3%A7%C3%A3o-do-reconhecimento -facial-no-setor-p%C3%BAblico.pdf. Acesso em: 9 mar. 2022.

FROOMKIN, A. Michael. The death of privacy? **Stanford Law Review**, [Stanford], v. 52, p. 1461-1543, May 2000. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2715617. Acesso em: 8 mar. 2022.

GATES, Kelly. Can computers be racist? **Juniata Voices**, [Huntingdon], v. 15, p. 5-17, 11 Sept. 2014. Disponível em: https://www.juniata.edu/offices/juniata-voices/media/volume-15/vol15-Gates.pdf. Acesso em: 5 mar. 2022.

GRINOVER, Ada Pellegrini. Processo penal transnacional: linhas evolutivas e garantias processuais. **Revista Brasileira de Ciências Criminais**, São Paulo, v. 9, p. 40-83, jan./mar. 1995.

GROTHER, Patrick *et al*. **Face recognition vendor test (FRVT)**: part 7: identification for paperless travel and immigration. [Gaithersburg]: NISTIR; [Washington, DC]: U.S. Department of Commerce, July 2021. Disponível em: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=932484. Acesso em: 10 mar. 2022.

GROTHER, Patrick; NGAN, Mei; HANAOKA, Kayee. **Face recognition vendor test (FRVT)**: part 3: demographic effects. [Gaithersburg]: NISTIR; [Washington, DC]: U.S. Department of Commerce, Dec. 2019. Disponível em: https://www.govinfo.gov/content/pkg/GOVPUB-C13-5a5c1d28d99c5a718d50bdbbae85cbb9/pdf/GOVPUB-C13-5a5c1d28d99c5a718d50bdbbae85cbb9.pdf. Acesso em: 5 mar. 2022.

INSTITUTO IGARAPÉ. **Reconhecimento facial no Brasil**. [Rio de Janeiro]: Instituto Igarapé, c2022. Disponível em: https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/. Acesso em: 2 mar. 2022.

JAIN, Anil K.; PANKANTI, Sharath. Beyond fingerprinting: security systems based on anatomical and behavioral characteristics may offer the best defense against identity theft. **Scientific American**, [*s. l.*], v. 299, n. 3, p. 78-81, Sept. 2008. Disponível em: http://biometrics.cse.msu.edu/Publications/GeneralBiometrics/JainPankanti_Beyond%20Fingerprinting_SCAM08.pdf. Acesso em: 3 mar. 2022.

KLARE, Brendan F. *et al*. Face recognition performance: role of demographic information. **IEEE Transactions on Information Forensics and Security**, [*s. l.*], v. 7, n. 6, p. 1789-1801, Dec. 2012. Disponível em: https://apps.dtic.mil/sti/pdfs/ADA556941.pdf. Acesso em: 4 mar. 2022.

KLONTZ, Joshua C.; JAIN, Anil K. A case study of automated face recognition: the Boston Marathon bombings suspects. **Computer**, [*s. l.*], v. 46, n. 11, p. 91-94, Nov. 2013. Disponível em: http://biometrics.cse.msu.edu/Publications/Face/KlontzJain_IEEEComputerNov2013.pdf. Acesso em: 4 mar. 2022.

LEMOS, Alessandra *et al*. **Comentários ao Anteprojeto de Lei de Proteção de Dados para a Segurança Pública**: tecnologia de reconhecimento facial. [Rio de Janeiro]: Instituto de Tecnologia & Sociedade do Rio, mar. 2021. Disponível em: https://itsrio.org/pt/publicacoes/comentarios-ao-anteprojeto-de-lei-de-protecao-de-dados-para-a-seguranca-publica/. Acesso em: 8 mar. 2022.

LESLIE, David. **Understanding bias in facial recognition technologies**: an explainer. [Londres]: The Alan Turing Institute, 2020. Disponível em: https://www.turing.ac.uk/sites/default/files/2020-10/understanding_bias_in_facial_recognition_technology.pdf. Acesso em: 3 mar. 2022.

LESSA, Luiz Fernando Voss Chagas. Notas sobre a evolução da cooperação internacional em matéria penal pelo Ministério Público Federal. *In:* BRASIL. Ministério Público Federal. Secretaria de Cooperação Internacional. **Temas de cooperação internacional**. 2. ed., rev. e atual. Brasília, DF: MPF, 2016. (Coleção MPF Internacional, 2). p. 117-124. Disponível em: https://memorial.mpf.mp.br/es/vitrine-virtual/publicacoes/temas-de-cooperacao-internacional-2a-edicao-revista-e-ampliada. Acesso em: 2 mar. 2022.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (org.). **LGPD**: Lei Geral de Proteção de Dados comentada. 2. ed. rev., atual. e ampl. São Paulo: Thomson Reuters Brasil, 2020. *E-book*.

MARKETSANDMARKETS. **Facial recognition market worth $8,5 billion by 2025**. [*S. l.*]: MarketsandMarkets, Dec. 2020. Disponível em: https://www.marketsandmarkets.com/PressReleases/facial-recognition.asp. Acesso em: 10 mar. 2022.

MATA, Federico Bueno de. Biometría e investigación criminal. **Revista Eletrônica de Direito Processual**, Rio de Janeiro, ano 14, v. 21, n. 3, p. 121-134, set./dez. 2020. Disponível em: https://www.e-publicacoes.uerj.br/index.php/redp/article/view/54200. Acesso em: 3 mar. 2022.

MENA, Isabela. **Verbete draft**: o que é reconhecimento facial. [*S. l.*]: Projeto Draft, 30 maio 2018. Disponível em: https://www.projetodraft.com/verbete-draft-o-que-e-reconhecimento-facial/. Acesso em: 3 mar. 2022.

MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. **Pensar Revista de Ciências Jurídicas**, Fortaleza, v. 25, n. 4, p. 1-18, out./dez. 2020.

MENDES, Laura Schertel Ferreira; MATTIUZZO, Marcela. Discriminação algorítmica: conceito, fundamento legal e tipologia. **Direito Público**, Porto Alegre, v. 16, n. 90, nov./dez. 2019. Assunto Especial – Doutrina, p. 39-64. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3766. Acesso em: 7 mar. 2022.

MILAJ, Jonida; BONNICI, Jeanne Pia Mifsud. Unwitting subjects of surveillance and the presumption of innocence. **Computer Law & Security Review**, [*s. l.*], v. 30, n. 4, p. 419-428, Aug. 2014.

MORAES, Maria Celina Bodin de; QUEIROZ, João Quinelato de. Autodeterminação informativa e responsabilização proativa: novos instrumentos de tutela da pessoa humana na LGPD. *In*: PROTEÇÃO de dados pessoais: privacidade versus avanço tecnológico. Rio de Janeiro: Fundação Konrad Adenauer, out. 2019. p. 113-135. (Cadernos Adenauer, 3).

NUNES, Fernanda Todesco *et al*. Um estudo sobre técnicas de biometria baseadas em padrões faciais e sua utilização na segurança pública. *In:* SPANHOL, Fernando José; LUNARDI, Giovani Mendonça;

SOUZA, Márcio Vieira de (org.). **Tecnologias da informação e comunicação na segurança pública e direitos humanos**. São Paulo: Blucher, 2016. (Coleção mídia, educação, inovação e conhecimento, v. 2). p. 113-131.

QUATTROCOLO, Serena. An introduction to AI and criminal justice in Europe. **Revista Brasileira de Direito Processual Penal**, Porto Alegre, v. 5, n. 3, p. 1519-1554, set./dez. 2019. Disponível em: http://www.ibraspp.com.br/revista/index.php/RBDPP/article/view/290/193. Acesso em: 8 mar. 2022.

ROYAL COURTS OF JUSTICE. Court of Appeal (Civil Division). **[2020] EWCA Civ 1058**. London: Royal Courts of Justice, 11 Aug. 2020. Disponível em: https://www.statewatch.org/media/1285/uk-court-of-appeal-bridges-v-swp-facial-rec-judgment-11-8-20.pdf. Acesso em: 12 mar. 2022.

SAADI, Ricardo Andrade. O crime organizado e a cooperação internacional. *In:* BRASIL. Ministério Público Federal. Secretaria de Cooperação Internacional. **Temas de cooperação internacional**. 2. ed., rev. e atual. Brasília, DF: MPF, 2016. (Coleção MPF Internacional, 2). p. 141-146. Disponível em: https://memorial.mpf.mp.br/es/vitrine-virtual/publicacoes/temas-de-cooperacao-internacional-2a-edicao-revista-e-ampliada. Acesso em: 2 mar. 2022.

SATO, Atsushi *et al*. Advances in face detection and recognition technologies. **NEC Journal of Advanced technology**, [*s. l.*], v. 2, n. 1, Winter 2005. Detection and Recognition Technologies, p. 28-34. Disponível em: https://www.nec.com/en/global/techrep/journal/g05/n01/pdf/a028.pdf. Acesso em: 6 mar. 2022.

SOUZA, Artur de Brito Gueiros. Terrorismo e cooperação penal internacional: desafios ao direito de extradição. *In:* BRASIL. Ministério Público Federal. Secretaria de Cooperação Internacional. **Temas de cooperação internacional**. 2. ed., rev. e atual. Brasília, DF: MPF, 2016. (Coleção MPF Internacional, 2). p. 163-176. Disponível em: https://memorial.mpf.mp.br/es/vitrine-virtual/publicacoes/temas-de-cooperacao-internacional-2a-edicao-revista-e-ampliada. Acesso em: 2 mar. 2022.

THE FACIAL recognition world map: smile, you're on camera. [*S. l.*]: Surfshark, mar. 2020. Disponível em: https://surfshark.com/facial-recognition-map. Acesso em: 5 mar. 2022.

UNIÃO EUROPEIA. Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho. **Jornal Oficial da União Europeia**: Bruxelas, n. L119, p. 89-131, 4 maio 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L0680&rid=1. Acesso em: 11 mar. 2022.

UNIVERSIDADE DE BRASÍLIA. Centro de Apoio ao Desenvolvimento Tecnológico. Laboratório de Tecnologias da Tomada de Decisão. **RT das 6 (seis) biometrias prováveis de utilização no RIC**. Brasília, DF: UnB, 2014. Disponível em: https://www.gov.br/mj/pt-br/acesso-a-informacao/governanca/pdfs/biometria-e-controle/20140610-mj-ric-rt-das-6-seis-biometrias-provaveis-de-utilizacao-no-ric.pdf. Acesso em: 5 mar. 2022.

VALENTE, Manuel Monteiro Guedes. Cooperação judiciária em matéria penal no âmbito do terrorismo. **Sistema Penal e Violência**, Porto Alegre, v. 5, n. 1, p. 73-92, jan./jun. 2013.

VALENTE, Manuel Monteiro Guedes. Editorial dossiê "Investigação preliminar, meios ocultos e novas tecnologias". **Revista Brasileira de Direito Processual Penal**, Porto Alegre, v. 3, n. 2, p. 473-482, maio/ago. 2017.

VIOLA, Mario; HERINGER, Leonardo; CARVALHO, Celina. **O anteprojeto da LGBT penal e as regras sobre transferência internacional de dados pessoais**. [Rio de Janeiro]: Instituto de Tecnologia & Sociedade do Rio, ago. 2021. Disponível em: https://itsrio.org/pt/publicacoes/o-anteprojeto-da-lgpd-penal-e-as-regras-sobre-transferencia-internacional-de-dados-pessoais/. Acesso em: 9 mar. 2022.

WERNECK, Antônio. Reconhecimento facial falha em segundo dia, e mulher inocente é confundida com criminosa já presa. **O Globo**, Rio de Janeiro, 11 jul. 2019. Disponível em: https://oglobo.globo.com/rio/reconhecimento-facial-falha-em-segundo-dia-mulher-inocente-confundida-com-criminosa-ja-presa-23798913. Acesso em: 3 mar. 2022.

ZAVASCKI, Teori Albino. Cooperação jurídica internacional e a concessão de exequatur. **Revista de processo**, São Paulo, v. 35, n. 183, p. 9-24, maio 2010.

ZUBOFF, Shosana. **A era do capitalismo de vigilância**: a luta por um future humano na nova fronteira do poder. Tradução de George Schelsinger. Rio de Janeiro: Intrínseca, 2020.

ZYLBERMAN, Joris. China chega à fase final de sistema de avaliação de cidadãos e preocupa ocidente. **UOL**, [*S. l.*], 2 jan. 2020. Notícias. Disponível em: https://noticias.uol.com.br/ultimas-noticias/rfi/2020/01/02/china-chega-a-fase-final-de-sistema-de-avaliacao-de-cidadaos-e-preocupa-ocidente.htm. Acesso em: 4 mar. 2022.