PARA A SUA SEGURANÇA, VOCÊ ESTÁ SENDO GRAVADO: O RECONHECIMENTO FACIAL SOB A LACUNA DA LEI DE Nº 13.709/18 NO ÂMBITO DA SEGURANÇA PÚBLICA

Victória Maria Bezerra Pereira[*]

Clara Cardoso Machado Jaborandy[**]

Resumo: O objetivo geral do presente artigo científico monta na utilização do mecanismo de reconhecimento facial no âmbito da segurança pública brasileira, em face da lacuna apresentada pela Lei Geral de Proteção de Dados (nº 13.709/18) acerca da temática. A pesquisa traz, em seu primeiro capítulo, a conceituação de inteligência artificial e reconhecimento facial, relacionando-os com o seu uso no âmbito da segurança pública e o disposto acerca desta seara na Lei de nº 13.709/18. Apresenta-se, portanto, a lacuna legislativa deixada pela referida lei, no tocante ao uso de dados biométricos pelo Estado, sob argumento de necessidade à segurança da sociedade. Ainda, exemplifica dispositivos pertinentes sobre o tema, como a Emenda de nº 17/2019, Marco Civil (nº 12.965/14) e o Marco Regulatório da Inteligência Artificial, Projeto de nº 21/2020. Em seu segundo capítulo, o presente trabalho traz os objetivos trazidos com a implantação do videomonitoramento no Brasil, exemplifica, através da observância de casos concretos, os motivos pelos quais atualmente inexistem restrições quanto ao uso da alusiva tecnologia, e, por fim, traz as possibilidades de sua utilização na hipótese de serem respeitados os preceitos constitucionais da privacidade,

[*] Graduada em Direito pela Universidade Tiradentes (2022). Advogada.
[**] Doutora e Mestre em Direito pela Universidade Federal da Bahia (UFBA). Professora do Programa de Pós-Graduação em Direitos Humanos da Universidade Tiradentes (UNIT/SE). Advogada.

intimidade e não discriminação. Para responder a indagação, será utilizada a metodologia dedutiva, juntamente de pesquisas bibliográficas, relacionando-as com o estudo de casos concretos, que indicam a ausência de viabilidade da Lei de nº 13.709, conter os avanços tecnológicos do reconhecimento facial que se contraponham aos direitos fundamentais dos cidadãos.

Palavras-Chave: Inteligência Artificial; Reconhecimento Facial; Lei Geral de Proteção de Dados; Segurança Pública; Privacidade.

Abstract: The general objective of this scientific article is based on the use of the facial recognition mechanism in the context of Brazilian public security, given the gap presented by the General Data Protection Law (No. 13.709 / 18) on the subject. The research brings, in its first chapter, the conceptualization of artificial intelligence and facial recognition, relating them to their use in the context of public security and the related aspect of this field in Law nº 13.709 / 18. legislative gap left by the law, regarding the use of biometric data by the State, under the argument of necessity for the security of society. It also exemplifies relevant provisions on the subject, such as Amendment No. 17/2019, Marco Civil (No. 12.965 / 14) and the Regulatory Framework for Artificial Intelligence, Project No. 21/2020. In its second chapter, this work brings the objectives brought about with the implementation of video surveillance in Brazil, exemplifies, through the observation of specific cases, the reasons why currently there are no restrictions on the use of the allusive technology, and, finally, it brings the possibility of its use in the event that the constitutional precepts of privacy, intimacy and non-discrimination are respected. To answer the question, the deductive methodology will be used, together with bibliographic research, relating them to the study of specific cases, which indicates the absence of feasibility of Law No. 13.709, containing

technological advances in facial recognition that oppose rights citizens' fundamentals.

Keywords: Artificial intelligence; Facial recognition; General Data Protection Law; Public security; Privacy.

INTRODUÇÃO

Consoante relatório confeccionado pelo Colégio Nacional de Defensores Públicos Gerais (Condege) juntamente com a Defensoria Pública do Rio de Janeiro (DPE-RJ), no período de 2012 a 2020 foram realizadas no mínimo noventa prisões injustas, através da tecnologia do reconhecimento facial. (CONDEGE, 2021).

A partir desse dado, faz-se necessário recordar a forma como se opera o algoritmo da biometria facial e quais são os seus reflexos na sociedade como um todo.

Em primeiro lugar, realiza-se a captura da face humana, com base em suas individualidades e simetrias, levando-se em conta elementos como o contorno, formato dos olhos, boca, cicatrizes, textura da pele e demais elementos. Em segundo lugar, os algoritmos presentes no sistema reúnem todas as características que possibilitam a obtenção de um padrão daquele rosto. Posteriormente, as informações coletadas são postas em comparação com banco de dados preexistente, a fim de possibilitar a identificação.

Assim como todo procedimento digital, o sistema de reconhecimento facial não é isento de falhas, vez que entre o processamento de coleta e resultado identificação, perpassam algoritmos e correspondências que fogem do poder do controlador dos aparelhos. A KeyApp, tecnologia já implementada em entidades públicas dos estados do Rio de Janeiro e Minas Gerais, apresenta índice de precisão de 90,98%. (BARROS, 2021).

Nessa perspectiva, muito embora a implementação do sistema de reconhecimento facial vise maior proteção aos cidadãos, bem como auxiliar os órgãos de segurança pública no processamento de diligências cotidianas e combate à criminalidade, é imprescindível que a sua utilização seja feita em grande zelo, tanto no processo de acolhimento do dado, quanto na utilização posterior deste, tendo em vista a probabilidade de erros, armazenamento e utilização incorreta, possível vazamento em massa de conteúdo tão sensível como é a feição e características físicas de cada cidadão.

É evidente que o uso inadequado e desmedido do reconhecimento facial acarreta graves consequências, como a violação à proteção de dados pessoais frágeis e o desrespeito aos princípios da não discriminação, privacidade e intimidade, tutelados constitucionalmente.

Nesse liame, importa mencionar que a Emenda de nº 17/2019, aprovada pelo Senado Federal em 20/10/2021, forneceu ao direito a proteção de dados pessoais, o status de direito fundamental, sendo imprescindível que os elementos intrínsecos a esse direito sejam protegidos não só na redação das normas, como também na prática. (BRASIL, Constituição (1998)).

Acerca de legislações sobre a temática, cabe destacar que a Lei Geral de Proteção de Dados (nº 13.709), publicada no ano de 2018, trouxe a biometria facial como dado sensível, ou seja, aquele em que demanda maior proteção constitucional, tendo em vista a plena exposição da intimidade e privacidade do identificado, e a sua vulnerabilidade à luz da possibilidade de discriminação negativa. (BRASIL, 2018).

Contudo, a despeito de assegurar o dado biométrico como sensível, em seu artigo 4º, inciso III, alínea "a", aduz que a legislação não se aplica ao uso e tratamento de dados pessoais no âmbito da segurança pública. Ainda, dispõe no parágrafo segundo que, posteriormente, em legislação específica, será tutelado o uso e tratamento de dados com a finalidade de segurança

pública. Atualmente o Estado caminha com o uso de inteligência artificial, porém com a ausência de legislação específica sobre o tema. (BRASIL, 2018).

À vista da lacuna deixada pela Lei Geral de Proteção de Dados, outros caminhos surgem com a finalidade de proteger a privacidade, intimidade, asseverar a não auto discriminação. Tem-se como exemplo o Marco Regulatório da Inteligência Artificial (IA), Projeto de Lei de nº 21/2020, aprovado pela Câmara dos Deputados em 29/9/2021, que busca regulamentar o uso de tecnologias artificiais na seara da segurança pública. (BRASIL, 2021). O Projeto aguarda votação no Senado Federal, para possivelmente se tornar vigente.

Diante do exposto, o presente artigo busca inicialmente tratar sobre os conceitos básicos do mecanismo de reconhecimento facial. Além disso, dispõe o que a Lei Geral de Proteção de Dados traz sobre o uso de dados sensíveis, como o dado biométrico. Ademais, após exemplificar a lacuna deixada pela Lei de nº 13.709/18, apresenta a necessidade de legislações que versem sobre a utilização da inteligência artificial no âmbito da segurança pública, em consonância com dispositivos que já caminham para tratar especificamente sobre o tema como o Marco Regulatório da Inteligência Artificial, projeto de Lei de nº 21/2020.

No segundo tópico, objetiva-se, exemplificar quais são os objetivos para a implementação do reconhecimento facial nos órgãos de segurança pública. Posteriormente, através de casos concretos, é demonstrado que diante da ausência de legislação específica sobre a temática, o Estado tem atuado juntamente com a inteligência artificial de modo irrestrito, gerando como consequência impactos que chegam a ferir princípios basilares como o da intimidade, privacidade, não auto discriminação e dignidade humana. Por fim, busca-se delinear que não há como conter os avanços trazidos pelo uso de inteligência artificial, porém, é possível que esta seja usufruída de modo que se garanta a

segurança da sociedade, sem tirar dela nos seus direitos fundamentais.

Ao final, conclui-se que o Estado tem se posicionado de maneira desmedida quanto ao uso do videomonitoramento, amparado na Lei Geral de Proteção de Dados que nada versa sobre limites pelos quais os órgãos devem seguir ao realizarem o uso da alusiva tecnologia.

Desse modo, constata-se a imprescindibilidade e urgência de legislação específica e apensa a Lei de nº 13.709/18, para que o reconhecimento facial seja utilizado, no âmbito da segurança pública, de modo restrito, seguro, preciso e sem apresentar violações aos direitos fundamentais.

Para tanto, essa pesquisa bibliográfica faz uso do método de abordagem qualitativo, auxiliada por publicações como bibliografias de autores renomados, pesquisas científicas, análise de legislações e casos concretos para o alcance da finalidade acima exposta.

"ARTIFICIAL INTELLIGENCE" SOB À ÉGIDE DA LEI GERAL DE PROTEÇÃO DE DADOS E SEGURANÇA PÚBLICA

O uso das tecnologias de inteligência artificial intensificou-se nos últimos anos, tendo em vista que a sua proposta ousada em automatizar as decisões e agilizar a prestação dos serviços públicos chamou a atenção dos gestores, no sentido de que sua aplicação específica nas instituições do Estado traria soluções rápidas aos problemas mais comuns do cotidiano, bem como encurtaria as relações entre os cidadãos e o ente estatal. (BECK, BOFF, PIAIA, 2021, p. 3).

No Brasil, o uso da tecnologia do reconhecimento facial surge sob argumento de atender aos anseios trazidos na seara da segurança pública, visando maior proteção, vigilância e diminuição da criminalidade na sociedade contemporânea.

Isso porque, o reconhecimento facial é tecnologia capaz de prover acesso em áreas urbanas, que vai além dos limites físicos dos agentes públicos, além de possibilitar rapidamente a identificação do rosto de qualquer indivíduo que pela tecnologia perpasse, com base na análise de banco de dados pré-constituído.

Por meio de monitoramento e vigilância de cidades, o emprego de reconhecimento facial funciona com a submissão de fotos a algoritmos, com o intuito de identificar pontos da geometria facial, únicos para cada pessoa. Com uma base de dados ampla o suficiente, o sistema de monitoramento é capaz de identificar em tempo real transeuntes anônimos em logradouros públicos monitorados, através da comparação de pontos faciais registrado no banco de imagens. (CRIPPA, OLIVEIRA, HOLANDA, p. 6, 2021)

Porém, não se percebe que a vigilância e, mais precisamente, o reconhecimento facial, cria um paradoxo. O monitoramento constante de rostos e corpos em ruas, praças, avenidas, empresas públicas, e até privadas, gera uma incerteza e insegurança na vida das pessoas que são submetidas a esse tratamento. (BARROS, SILVA, 2020, p. 2)

Acerca do tratamento desses dados, a Lei Geral de Proteção de Dados (nº 13.709), em seu artigo 4º, inciso III, alínea "a", dispõe que esta legislação não se aplica ao tratamento de dados pessoais para fins exclusivamente de segurança pública. (BRASIL, 2018).

Além disso, ainda informa que "o tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei." (BRASIL, 2018).

Logo após, aduz: "§ 2º É vedado o tratamento dos dados a que se refere o inciso III do caput deste artigo por pessoa de

direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo.". (BRASIL, 2018).

É justamente o caso do reconhecimento facial no Brasil, pois inexiste sistema próprio do poder público nesse sentido — deverá haver um informe específico à ANPD (Autoridade Nacional de Proteção de Dados). (GOMES, 2020).

Nesse liame, cabe citar ainda que o Regulamento Geral de Proteção de Dados (GDPR, em sigla inglesa), legislação europeia que serviu de inspiração para a criação da Lei Geral de Proteção de Dados, também optou pela criação de legislação específica para o tratamento de dados voltados à segurança pública, o que fora providenciado de forma breve.

Em sentindo oposto, no Brasil, após dois anos da publicação da Lei nº 13.709/18, ainda não se observa legislação concernente ao uso de tecnologias artificiais na seara da segurança pública, o que não impossibilitou o seu uso. Nota-se que na ausência de normas específicas que delimitem as formas e os modos adequados de utilização do reconhecimento facial, este passa a ser usufruído de maneira irrestrita e conveniente ao Poder Público.

Desse contexto de lacuna legislativa é possível extrair três problemas fundamentais. O primeiro consiste na ausência de uniformidade nacional entre os sistemas de identificação criminal por reconhecimento facial em uso no país. (DE PAULA, CARDOSO, ARAÚJO, 2021, p. 4).

O segundo problema é a ausência de limites e diretrizes aos programadores e empresas privadas que comercializam os softwares no tocante a questões éticas, de transparência no tratamento dos dados, de privacidade dos vigiados, de limites ao compartilhamento de dados entre os atores da persecução penal e, em especial, a responsabilização por eventuais infrações aos postulados regulatórios. (DE PAULA, CARDOSO, ARAÚJO,

2021, p. 4).

Por fim, o terceiro e mais grave problema é a proteção deficiente dos cidadãos expostos às tecnologias de reconhecimento, aos quais não é dado saber como as suas informações chegaram até os bancos de dados. (DE PAULA, CARDOSO, ARAÚJO, 2021, p. 5).

Acontece que existem muitas formas de como o reconhecimento facial pode prejudicar as pessoas, principalmente aplicado à segurança pública. Historicamente, a vigilância do governo foi (e ainda é) direcionada desproporcionalmente às comunidades marginalizadas, principalmente imigrantes, pobres, minorias étnicas e negros. (HARTZOG, SELINGER, 2020, p. 4-5).

Não obstante, o tratamento dos dados pelo setor público encontra respaldo na facilidade de realizar estudos sobre a população e no controle social, não olvidando da existência de limitações que o próprio sistema jurídico estabelece para assegurar a proteção dos direitos fundamentais individuais, no entanto, em determinadas situações como a de uma pandemia podem instigar a relativização do direitos, bem como violação dos mesmos. (BECK, BOFF, PIAIA, 2021, p. 8).

Outro ponto importante à ser destacado é que além da ausência de regulamentação específica nacional, o país caminha para fornecer aos Estados autonomia suficiente para utilizar a tecnologia do reconhecimento facial como desejem. Francisco, Hurel, Rielli (2020, p. 19), afirmam que "Assim como ocorre nos EUA, o Brasil vem optando por uma regulação nos âmbitos estaduais. Isso permite maior experimentação e garante que os entes federativos incorporem suas particularidades na observância dos princípios". Ocorre que, conforme os autores supracitados aduzem:

> A ausência de uma legislação única, ou de um órgão central que faça a fiscalização do emprego dos sistemas de reconhecimento facial dificulta a observância dos princípios, de modo que violações a direitos e garantias individuais possam ocorrer

> sem a devida responsabilização. (Francisco, Hurel, Rielli, 2020, p. 19).

Isso significa que, voluntária ou involuntariamente, vivemos sob o constante monitoramento possibilitado pelo avanço tecnológico. Voluntariamente, pois em diversas ocasiões cedemos "livremente" nossos dados pessoais ao governo e a corporações privadas; involuntariamente, pois em diversas outras encontramo-nos ostensivamente vigiados, sem que a nós seja dada a oportunidade de consentirmos no que diz respeito a tal vigilância. (NEGRI, OLIVEIRA, COSTA, 2020, p. 91).

Nesse sentido, a abordagem brasileira oferece poucas garantias para coibir os potenciais riscos aos direitos e garantias individuais gerados pelo emprego de sistemas de reconhecimento facial. Ainda que o país tenha se esforçado para construir sua Lei Geral de Proteção de Dados, é fundamental buscar a instrumentalização dos princípios nela apresentados. (FRANCISCO, HUREL, RIELLI, 2020, p. 20).

Consoante será delimitado no presente artigo, faz-se imprescindível a publicação de legislação que verse exclusivamente sobre o uso de tecnologias artificiais voltadas a manutenção da seguridade nacional, se não, consoante argumenta o autor Rennes (2019) "sob o argumento de se concretizar a segurança estatal, a chamada proteção de dados pessoais, que muitas vezes deveriam ser açambarcada pela inviolabilidade da privacidade e intimidade, poderá ser representada metaforicamente por um frágil teto de vidro.".

Atualmente, nota-se que a Lei de nº 13.706/18, demonstra-se insuficiente para determinar os limites pelos quais as tecnologias de reconhecimento facial devem ser utilizadas no âmbito da segurança pública, sob a égide da primazia do interesse público, em sentido oposto às garantias constitucionais como os direitos da privacidade, intimidade e da auto não discriminação.

Importa aduzir que com o advento da Emenda ao texto constitucional de nº 17/2019, aprovada pelo Senado Federal em 20/10/2021 (BRASIL, 2021), o direito a proteção de dados

pessoais ganha o status de direito fundamental, sendo assim, imprescindível que todo o contexto que envolve a proteção de dados pessoais deva ser realizado com clareza e pugnando pela inviolabilidade da privacidade e intimidade de todos os cidadãos.

Ainda, vale dizer que não obstante a ausência de legislação apensa à Lei de nº 13.706/18, que verse sobre os limites de tratamento de dados no âmbito da segurança pública, a Câmara dos Deputados aprovou, em 29/9/2021, com 413 votos a favor e 15 contra, o Projeto de Lei de nº 21/2020, que gera o Marco Regulatório da Inteligência Artificial (IA). (BRASIL, 2021)

Acerca desse ponto, vale dizer que no texto houve mudanças no artigo 4º, que define os fundamentos do desenvolvimento e aplicação de inteligência artificial no Brasil. Um dos incisos adicionados diz que é preciso haver a harmonização com a LGPD, o Marco Civil da Internet, o Sistema Brasileiro de Livre Concorrência e o Código de Defesa do Consumidor. Outro inciso diz que o desenvolvimento de IA deve ter como fundamento a segurança, a privacidade e a proteção de dados pessoais. (OYAMA, 2021).

Além disso, os agentes de IA terão uma série de deveres, como responder, legalmente, pelas decisões tomadas por um sistema de inteligência artificial e assegurar que os dados utilizados respeitam a Lei Geral de Proteção de Dados (LGPD). A norma regula o tratamento de dados pessoais de clientes e usuários de empresas do setor público e privado. (VIANA, 2020). O referido projeto atualmente segue para o Senado Federal em busca de completa aprovação.

Soma-se a isso o fato de que, em 2019, o então ministro da segurança pública assinou a Portaria nº 793, a qual previa o fomento à implantação de sistemas de videomonitoramento com soluções de reconhecimento facial, mediante financiamento do Fundo Nacional de Segurança Pública (BRASIL, 2019). Isto posto, fica evidente que a análise a respeito da viabilidade de utilização do reconhecimento facial é urgente, pois já há registos

de sua implementação e até mesmo de prisões realizadas através dele. (DE PAULA, CARDOSO, ARAÚJO, 2021, p. 9)

Por esse motivo, faz-se ainda mais imprescindível que surja regulamentação que verse especificamente sobre o uso de dados pessoais e sensíveis na seara da segurança pública, em conjunto ao uso da inteligência artificial voltada a seguridade nacional, de modo que todos os esforços para implementação tanto da Lei Geral de Proteção de Dados, quanto da Emenda supracitada sejam aplicados na prática, a fim de resguardar a privacidade, intimidade e não discriminação.

"ARTIFICIAL INTELLIGENCE": LIMITES E POSSIBILIDADES DE UTILIZAÇÃO NA SEGURANÇA PÚBLICA

Os dispositivos de reconhecimento facial na área de segurança pública foram oficialmente inaugurados no Brasil em 2019. De acordo com a Portaria nº 793 de outubro de 2019, em seu capítulo 4, inciso 1º, letra b, o Governo Federal autorizou o uso do Fundo Nacional de Segurança Pública no "fomento à implantação de sistemas de videomonitoramento com soluções de reconhecimento facial" como medida de enfrentamento à criminalidade violenta. Contudo a tecnologia ainda apresenta muitas dúvidas e controvérsias. (BEZERRA, MAGNO, 2020, p. 4)

O referido sistema de captação via reconhecimento facial registra a face do cidadão, para, posteriormente, colocar em comparação com banco de dados preexistentes, com o fito de localizar a sua identidade e demais características, sejam elas físicas ou alusivas aos seus dados pessoais.

Contudo, Madja e Josenildo (2020, p. 7) aduzem: A tecnologia não é neutra. O algoritmo é uma representação social. Trata-se de um dispositivo em uma rede de relações estratégicas e sobredeterminadas que, por meio de sistemas matemáticos ou de inteligência artificial, mediam informações que alimentam e regem seu funcionamento de disciplinaridade dos corpos.

Em virtude da neutralidade distante, a implantação e funcionamento do sistema de videomonitoramento acaba por retratar padrões e características físicas pelas quais a sociedade já visualiza a necessidade de vigilância e imposição de sanções, originando o que se denomina, atualmente, de racismo algorítmico[1]. Fato que não é surpresa, vez que por trás de todo sistema, existe um ou mais indivíduos que o programam para que funcione como a mente humana. Dessa forma, nota-se a facilidade em replicar comportamentos já reiterados na sociedade às máquinas.

Deve-se destacar ainda, que não somente as câmeras e demais utilitários para captação das imagens e vídeos possuem papel fundamental no processamento das informações, como também é de suma importância que o banco de dados esteja regularmente atualizado, para que o comparativo imagem-dado seja realizado de modo eficaz e preciso.

Assim, nota-se que o sistema de reconhecimento facial no Brasil apresenta captação pouco rigorosamente. Isso porque, consoante exposto acima, atualmente não há legislação que verse especificamente sobre os limites pelos quais o Estado deve respeitar, para aplicação da referida tecnologia.

Os projetos de reconhecimento facial têm se baseado na instalação de câmeras que capturam imagens 24 horas em ruas, terminais rodoviários e estações de metrô, aliados a algoritmos que processam um número altíssimo de imagens de rostos combinando com bancos de dados diversos, muitas vezes sem o conhecimento do público. O potencial de dano é muito maior, uma vez que milhares de pessoas são escaneadas por hora. Para se ter ideia, a primeira fase do projeto de reconhecimento facial em Copacabana capturou 3 milhões de faces. (NUNES, 2021).

Em razão disso, o país já apresenta impactos desastrosos na sociedade, vez a natureza sensível do que é extraído com o

[1] *SILVA, Tarcízio*. Racismo Algorítmico em Plataformas Digitais: microagressões e discriminação em código. Anais do VI Simpósio Internacional LAVITS. Salvador (Bahia), Brasil, 2019b.

uso do reconhecimento facial, a relação com a segurança pública e a linha tênue entre proteção e violação à dignidade humana, princípio basilar protegido constitucionalmente.

Através das câmeras que realizam o reconhecimento facial de toda a população, os órgãos designados à segurança pública brasileira desenvolvem um olhar sem rosto. A partir do uso delas, não só faces são detectadas a todo momento, como também são registradas todas as condutas tomadas pelos cidadãos, criando assim, verdadeiro modelo de monitoramento e vigilância, que perpassa o adequado, diante da existência de fundamentos constitucionais que resguardam a intimidade e a privacidade do indivíduo.

A partir dessa análise e da ausência de uma legislação específica para o tema, questiona-se quais são os limites atuais, impostos ao Poder Público, de modo a permitir que o videomonitoramento seja realizado, ao tempo em que sejam resguardados os preceitos constitucionais inerentes a todos os cidadãos.

Nesse sentido, cabe exemplificar o funcionamento do reconhecimento facial no país de forma ampla, com enfoque na segurança pública, de forma a observar que desde a sua implementação, são inúmeras as situações em que se observa o uso irrestrito e desmedido do videomonitoramento.

Aqui no Brasil, esta tecnologia passou a ser mais discutida a partir de abril de 2018 quando um sistema de reconhecimento facial foi instalado na linha vermelha do Metrô de São Paulo. O sistema mudava anúncios exibidos aos passageiros conforme suas expressões faciais. Era possível detectar idade e sexo e classificar as emoções nas categorias feliz, insatisfeito, surpreso ou neutro. Desenvolvido pela empresa Via Quatro, o projeto foi implementado em conjunto com a LG, companhia multinacional de eletrônicos que forneceu as telas, e com a Hypera Pharma, uma grande empresa farmacêutica brasileira. (TAUTE, 2020)

Logo após ampla discussão sobre o caso, que gerou a

Ação Civil imposta pelo Instituto Brasileiro de Defesa do Consumidor (IDEC) em desfavor da empresa Via Quatro, o Judiciário determinou a cessação da coleta de dados, em virtude da ausência de consentimento dos transeuntes e passageiros.

Contudo, em julho de 2019, o Metrô de São Paulo reapareceu no noticiário ao instalar um novo sistema de monitoramento, aumentando o parque de câmeras extensivamente e dessa vez com a opção de vincular o sistema aos bancos de dados da Secretaria de Segurança Pública para perseguição de foragidos da Justiça. (TAUTE, 2020).

Não é difícil duvidar que haja realmente uma crise de segurança no Metrô para justificar o uso desse meio. O uso de fotografia de rostos de pessoas tem grande uso na história para a busca de criminosos e não apresentava questões éticas. Por outro lado a tecnologia de reconhecimento facial está ligada a bancos de dados gigantes que possibilitam não só um uso em processos criminais, mas como uma vigilância em massa, na qual não há diferenciação de quem está sendo monitorado. (TAUTE, 2020).

Importa destacar que muito embora não haja uma clara diferenciação de quem está sendo monitorado, o que se extraí da aplicação atual do referido sistema no país, é que em virtude da ausência de neutralidade, a tecnologia de reconhecimento facial não abrange completamente, em sua detecção, rostos que possuem tom de pele mais escuro, especialmente mulheres, grupos já vulneráveis socialmente.

Um dispositivo de reconhecimento facial foi aplicado na Bahia, no Rio de Janeiro, em Santa Catarina e na Paraíba e, segundo o Departamento Penitenciário Nacional, "foram detidas 108.395 pessoas, das quais 66.419 são negras ou pardas, um total de 61,27%", na clara evidência do preconceito racista do sistema criminal. (ARTUR, 2021). No MIT, pesquisadores identificaram que algoritmos para identificar o gênero com base no rosto classificaram mulheres de pele escura como homens em quase 35% das vezes. (MARASCIULO, 2020).

Em um levantamento feito nos estados da Bahia, Ceará, Pernambuco e Rio de Janeiro, entre cento e oitenta pessoas presas com o uso de reconhecimento, noventa por cento eram negras (NUNES, 2020).

Diante dos casos supramencionados, observa-se que a tecnologia de reconhecimento facial encontra o seu primeiro obstáculo: a precisão na captação das faces que por ela transitem. Contudo, não é somente essa a única questão enfrentada, sendo imprescindível citar as consequências causadas por um banco de dados desatualizado.

À título de ressalva, o banco de dados objetiva arquivar os rostos já cadastrados, para, posteriormente, ser utilizado em comparação com as faces captadas pelas câmeras. Ocorre que na hipótese de existir um banco de dados desatualizado, há grande possibilidade, por exemplo, das pesquisas resultarem em combinações entre pessoas diferentes.

Sob essa perspectiva, em julho de 2019, a polícia do Rio de Janeiro, ao iniciar o seu projeto de reconhecimento facial, reconheceu uma mulher como Maria Lêda Félix da Silva, condenada por homicídio. Imediatamente os policiais a conduziram a mulher, que dizia não ser a procurada, até a delegacia. Na ocasião, fora constatado que de fato, ela não era a pessoa almejada. Ainda, foi apurado que a mulher procurada em primeiro momento cumpria pena há cerca de quatro anos, dado não constatado vez que o banco de informações estava desatualizado. (NUNES, 2021).

Os especialistas apontam que, além da falta de informações sobre como os dados são gerenciados, os órgãos de segurança brasileiros não oferecem informações sobre a eficiência desses sistemas. Na Inglaterra, por exemplo, um levantamento encomendado pela polícia de Londres e realizado por pesquisadores da Universidade de Essex apontou que 81% dos alertas feitos pela ferramenta local estavam incorretos. (SILVA, 2021).

Nesse sentido, é pertinente exemplificar com a análise

feita pelo CESEC (NUNES, 2019, p. 88), com base nos dados do monitoramento na cidade de Feira de Santana, durante quatro dias da micareta de 2019: dos alertas emitidos, mais de 96% eram falsos. Foram 1,3 milhões de pessoas com seus rostos capturados, que geraram 903 alertas, dos quais resultou o cumprimento de 18 mandados de prisão e prisão de 15 pessoas. O alto índice de falsos positivos é alarmante e causa questionamentos sobre a eficiência na aplicação dessas tecnologias. Ademais, a abordagem adotada a partir dessas correspondências pode contribuir na propagação de injustiças. (GOMES, MAGALHÃES, 2021, p. 9).

Assim, observa-se que diante da ausência de legislação que verse, especificamente, sobre os limites no uso e tratamento de dados pessoais e sensíveis, especialmente no âmbito da segurança pública, o Estado passa a utilizar a referida tecnologia de inteligência artificial de modo irrestrito, sendo visível os danos já causados em virtude dessa conduta.

Outrossim, cabe dizer que o presente artigo não busca argumentar sobre a necessidade de não utilização da tecnologia de reconhecimento facial. Isso porque, os avanços em consequência de seu uso podem e devem ser considerados como válidos para um auxílio aos órgãos de segurança pública.

Entretanto, um bom uso da inteligência artificial está estritamente ligado ao respeito as normas constitucionais já vigentes. Por esse lado, faz-se importante destacar as possibilidades pelas quais o videomonitoramento pode ser utilizado, sem a violação dos princípios da intimidade, privacidade e não autodiscriminação.

No mesmo sentido, indispensável é o controle da fonte primária dos algoritmos. É dizer, os sujeitos responsáveis por sua elaboração e programação, enquanto capazes de influir no funcionamento do sistema, merecem atenção dos responsáveis, a fim de que essa influência não acabe por perpetuar pré-conceitos. (DE PAULA, CARDOSO, ARAÚJO, 2021, p. 11).

Nesse liame, a partir de uma norma regulamentadora específica, far-se-á possível o investimento, por parte do Estado, em softwares que atendam às necessidades em termos de qualidade e eficiência, no tocante à precisão do sistema utilizado para realização do monitoramento. Não obstante a isso, a capacitação das pessoas responsáveis pelo cruzamento de dados trazidos pelas câmera até os bancos de dados.

Indispensável, também, a existência de bancos de dados confiáveis e com frequente atualização, para que se evite, por exemplo, prisões como aquela no Rio de Janeiro, em que a verdadeira infratora já se encontrava encarcerada. (DE PAULA, CARDOSO, ARAÚJO, 2021, p. 11).

O uso de sistemas de inteligência artificial pelo poder público apresenta potencial tanto para ampliar a acurácia, justiça, transparência e efetividade nas tomadas de decisões quanto para tornar-se uma arma de destruição matemática, intensificando a discriminação e infringindo direitos. A escolha pela concretização deste ou daquele potencial, por sua vez, depende da identificação dos riscos decorrentes do uso irresponsável dessas tecnologias e da minimização desses por meio de mecanismos de governança. (GOMES, MAGALHÃES, 2021, p. 11)

À vista disso, cabe ressaltar que o mecanismo de governança apto a estabelecer limites adequados a utilização do reconhecimento facial, uma das possibilidades provenientes do uso de inteligências artificiais, seria uma legislação específica para o tema. Nesse sentido, considerando a ausência de lei apensa a Lei Geral de Proteção de Dados, tem-se como exemplo concreto, o Projeto de Lei de nº 21/2020, que gera o Marco Regulatório da Inteligência Artificial (IA). Na hipótese de sua aprovação posterior no Senado Federal e vigência, estima-se que os recursos tecnológicos sejam utilizados com mais prudência e perfazendo as linhas indispensáveis a não ferir nenhum preceito constitucional.

Nesse liame, o próprio Marco Regulatório traz em seu art. 4º, III, IV e V, como fundamento o respeito aos direitos

humanos e aos valores democráticos, a igualdade, a não discriminação, a pluralidade e o respeito aos direitos trabalhistas e a privacidade e a proteção de dados.

Assim, o presente artigo busca exemplificar que atualmente não se encontram artifícios jurídicos aptos a impor limites ao uso do reconhecimento facial no âmbito da segurança pública, dada a lacuna deixada pela Lei Geral de Proteção de Dados, a partir da citação de outras pesquisas científicas, dados e casos concretos, contudo, há a possibilidade do país caminhar para a utilização da referida tecnologia, com a construção de bases sólidas de softwares e banco de dados eficientes, juntamente com uma legislação que forneça as diretrizes necessárias a regulamentação desse avanço tecnológico tão necessário quando se trata de um âmbito sensível e que deve ser resguardado pelo Estado.

CONSIDERAÇÕES FINAIS

Em breve síntese, o presente trabalho científico almeja exemplificar o uso da inteligência artificial, através de reconhecimento facial, voltado à segurança pública, contrapondo-o com o disposto Lei Geral de Proteção de Dados acerca da temática.

Consoante visto, o videomonitoramento é tecnologia artificial dotada da capacidade de prover acesso em áreas urbanas externas e internas, que vai além dos limites físicos dos agentes de segurança pública, e possibilitam rapidamente a identificação de qualquer indivíduo que pela tecnologia perpasse, com base na análise de banco de dados pré-constituído.

Contudo, ainda não se observa na Lei Geral de Proteção de Dados, regulamentação concernente a coleta, tratamento e uso de dados pessoais extraídos da tecnologia supracitada no âmbito da segurança pública, o que não impossibilitou o seu uso.

O contexto exposto demonstra que é na ausência de regulamentações específicas, que o Poder Público passa a usufruir

e implantar a inteligência artificial de modo irrestrito e conveniente aos órgãos de segurança pública.

Isto posto, inicialmente a pesquisa retrata o objetivo do Estado com a implantação do videomonitoramento em espaços públicos, sob a visão da ausência de limites para com o seu uso e possibilidades de utilização com a segurança jurídica necessária, ambas pontuações relacionadas com o disposto na Lei de nº 13.709/18.

O atual trabalho ressalta o fator neutralidade, no sentido de exemplificar que o reconhecimento facial acaba por reproduzir padrões pelos quais a sociedade já visualiza necessidade de vigilância, o que se denomina racismo algoritmo. Devendo-se levar em consideração que todos os sistemas são programados a partir da mente humana, sendo facilmente replicados comportamentos humanos às maquinas.

Neste quadrante, a pesquisa constrói a argumentação que atualmente, o Estado, pautado na primazia do interesse público, se utiliza do sistema de videomonitoramento, sob a alegação de proteção de toda a sociedade.

Contudo, ao mesmo tempo, mitiga direitos fundamentais como a privacidade, intimidade, não auto discriminação, proteção de dados pessoais, tanto pela ausência de consentimento de uso e compartilhamento de um dado tão sensível quanto a imagem, quanto pela possibilidade de equívocos, originados por fatores como falta de precisão na captura da face humana ou banco de dados desatualizados, conforme observado na análise de casos concretos.

Nesse liame, muito embora a utilização do sistema de reconhecimento facial busque maior proteção aos cidadãos, bem como auxiliar os órgãos de segurança pública no processamento de diligências cotidianas e combate à criminalidade, é necessário que a sua implantação seja realizada com sistemas seguros e precisos, para o devido acolhimento, armazenamento e utilização posterior do dado sensível coletado.

Atualmente, a Lei nº 13.709/18 não é suficiente para conter os avanços realizados pela utilização do reconhecimento facial no âmbito da segurança pública, fazendo-se imprescindível que surja legislação apensa que regulamente de forma específica os meios, mecanismos e locais adequados para implementação e uso de inteligências artificiais, de modo a não violar preceitos constitucionais inerentes a todos os cidadãos.

REFERÊNCIAS

ARTUR, Margarete. Qual o impacto da tecnologia de reconhecimento facial na população negra? (2021). Disponível em: < https://jornal.usp.br/ciencias/qual-o-impacto-da-tecnologia-de-reconhecimento-facial-na-populacao-negra/ > Acesso em: 25/10/2021.

BARROS, Isabela. SILVA, Isabela. Utilização do reconhecimento facial eletrônico por empresas para identificação de suspeitos: segurança ou violação do estado democrático de direito?. Revista Transgressões Ciências Criminais em Debate. V.8, n.1, 2020.

BARROS, MATHEUS. EMPRESA PROMETE 99% DE PRECISÃO NO RECONHECIMENTO FACIAL DE NEGROS. .Disponível em: < https://olhardigital.com.br/2021/04/23/seguranca/empresa-brasileira-promete-99-de-precisao-no-reconhecimento-facial-de-negros/ > Acesso em: 23/04/2021.

BECK, Cesar Augusto; BOFF, Murilo; PIAIA, Thami. Os (ab)usos da tecnologia de reconhecimento facial na segurança pública e na prestação de serviços a partir da pandemia de covid-19. Revista Pensamento Jurídico. São Paulo. Vol.15. nº 2, 2021.

BESSI, Vania. Zimmer, Marco. GRISCI, Carmem. O PANÓPTICO DIGITAL NAS ORGANIZAÇÕES: ESPAÇO-TEMPORALIDADE E CONTROLE NO MUNDO DO TRABALHO CONTEMPORÂNEO. < https://www.nexojornal.com.br/ensaio/2020/Reconhecimento-facial-e-LGPD-uma-pol%C3%AAmica-para-o-s%C3%A9culo-21 >- v.14 - n.42, 2007. Acesso em: 04/11/2021.

BRASIL. Constituição (1988). Emenda constitucional nº 17, de 03 de julho de 2019. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=node01kdq4pv3xca60tu0uw9bb8a8r14120828.node0?codteor=1773684&filename=PEC+17/2019. Acesso em: 03/11/2021.

BRASIL. Lei Geral de Proteção de Dados (2018). Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm > Acesso em 03/11/2021.

BRASIL. Portaria nº 793, de 24 de outubro de 2019. Disponível em: < https://bit.ly/2KdhOZH > . Acesso em: 03/11/2021.

BRASIL. Projeto de Lei nº 21 (2021). Disponível em: < https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1853928 > Acesso em: 03/11/2021.

CRIPPA, Margarete Esteves. OLIVEIRA, Loryne. HOLANDA, Tamires. Uso do reconhecimento facial aplicado à segurança pública no Brasil (2021). Disponível em: < http://ojs.sociologia-alas.org/index.php/CyC/article/view/248/265 >.

CRUZ, Renne Muller. Análise do artigo 4º da Lei de Proteção de Dados (2019). Disponível em: < https://jus.com.br/artigos/71291/analise-do-artigo-4-da-lei-de-protecao-de-dados > Acesso em 16/10/2021.

DE PAULA, Amanda Marcélia. CARDOSO, Naiara Deperon. ARAÚJO, Romulo de Aguiar. Regulação e Uso do

Reconhecimento Facial na Segurança Pública do Brasil. Revista de Doutrina Jur, Brasília/DF, v. 112, eo21009, 2021. Disponível em: < https://revistajuridica.tjdft.jus.br/index.php/rdj/article/view/734/135 > Acesso em: 10/10/2021.

FRANCISCO, Pedro Augusto. HUREL, Louise. RIELLI, Mariana. Regulação do reconhecimento facial no setor público: avaliação de experiências internacionais. Instituto Igaripé. Data Privacy Brasil Research. 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 12/10/2021.

GOMES, Rodrigo Dias Pinho. Reconhecimento Facial e LGPD: uma polêmica para o século 21 (2020). Disponível em: < https://www.nexojornal.com.br/ensaio/2020/Reconhecimento-facial-e-LGPD-uma-pol%C3%AAmica-para-o-s%C3%A9culo-21 > Acesso em: 03/11/2021.

GOMES, Rodrigo Dias Pinho. Reconhecimento facial e LGPD: uma polêmica para o século 21 (2020). Disponível em: < https://www.nexojornal.com.br/ensaio/2020/Reconhecimento-facial-e-LGPD-uma-pol%C3%AAmica-para-o-s%C3%A9culo-21. 2021 |

GOMES, Técio Spínola. MAGALHÃES, Alice Azevedo. Regulação de Sistemas de Reconhecimento Facial para fins de segurança pública no Brasil: Riscos e Desafios (2021). Revista Humanidades e Inovação. V.8. n. 47. Disponível em: < file:///C:/Users/SAMSUNG/Downloads/5639-Texto%20do%20artigo-19978-1-10-20210929.pdf >. Acesso em: 22/10/2021.

HARTZOG, Woodrow; SELINGER, Evan. The Case for Banning Law Enforcement From Using Facial Recognition Technology. The Justice Collaborative Institute, Agosto de 2020. p. 4–5.

MAGNO, Madja. BEZERRA, Josenildo. Vigilância negra: o dispositivo de reconhecimento facial e a disciplinaridade dos corpos Revista Novos Olhares | Vol.9 N.2 | ago-dez/2020. file:///C:/Users/SAMSUNG/Downloads/165698-Texto%20do%20artigo-473296-1-10-20210302.pdf)

MARASCIULO, Marilia. Reconhecimento facial: prós e contras da tecnologia que veio para ficar (2020). Disponível em: < https://revistagalileu.globo.com/Tecnologia/noticia/2020/06/reconhecimento-facial-pros-e-contras-da-tecnologia-que-veio-para-ficar.html > Acesso em: 25/10/2021.

NEGRI, Sergio. OLIVEIRA, Samuel. COSTA, RAMON. O Uso de Tecnologias de Reconhecimento Facial Baseadas em Inteligência Artificial e o Direito à Proteção de Dados. RDP, Brasília, Volume 17, n. 93, 82-103, maio/jun. 2020.

NUNES, Pablo. Artigo: O algoritmo e racismo nosso de cada dia (2021). Disponível em: < https://cesecseguranca.com.br/artigo/o-algoritmo-e-racismo-nosso-de-cada-dia/ > Acesso em: 15/10/2021.

NUNES, Pablo. Uso de Reconhecimento facial na segurança pública no Brasil. In: SEMINÁRIO PROTEÇÃO DE DADOS E OS IMPACTOS SOCIAIS, 2020, Rio de Janeiro, Anais [...]. Disponível em: < https://www.youtube.com/watch?v=q7py8yePjqk&ab_channel=TVALERJ > Acesso em: 20/10/2021.

OYAMA, Érico. Câmara aprova Marco Regulatório da Inteligência Artificial (2021). Disponível em: < https://www.jota.info/legislativo/camara-aprova-marco-regulatorio-da-inteligencia-artificial-29092021 >. Acesso em: 20/10/2021.

Relatórios indicam prisões injustas após reconhecimento fotográfico. Disponível em: <

http://condege.org.br/2021/04/19/relatorios-indicam-prisoes-injustas-apos-reconhecimento-fotografico/. Acesso em: 10/10/2021

SILVA, Victor Hugo. Por que o uso de reconhecimento facial na segurança é controverso? (2021). Disponível em: < https://tecnoblog.net/380749/por-que-o-uso-de-reconhecimento-facial-na-seguranca-e-controverso/ > Acesso em: 20/10/2021.

TAUTE, Fabian. Reconhecimento Facial e suas controvérsias, 2020. Disponível em: < https://br.boell.org/pt-br/2020/02/05/reconhecimento-facial-e-suas-controversias > Acesso em: 20/10/2021.

VIANA, Cleia. *Projeto cria marco legal para uso de inteligência artificial no Brasil*, 2020. Disponível em: < https://www.camara.leg.br/noticias/641927-projeto-cria-marco-legal-para-uso-de-inteligencia-artificial-no-brasil/ > Acesso em: 25/10/2021.