Uso do reconhecimento facial aplicado à segurança pública no Brasil

Uso de reconocimiento facial aplicado a la seguridad pública en Brasil

Margarete Esteves Nunes Crippa
margarete.crippa@gmail.com
Loryne Viana de Oliveira. *loryne@ymail.com*
Itala Laurente. *itala.laurente@gmail.com*
Tamires Holanda. *tami.holanda@gmail.com*
Universidade Estadual de Campinas. Brasil
Recibido: 11/01/2021
Aprobado: 18/02/2021

Resumo
Reconhecimento facial é uma habilidade empregada cotidianamente em nossas vidas. Desde 1960, quando se iniciaram as pesquisas, até hoje, em um ritmo crescentemente acelerado, há interesse em viabilizar o processamento automatizado de imagens digitais para reconhecimento facial para uma ampla gama de aplicações, tais como: autenticação biométrica, vigilância, interação computador-humano, entre outros. Este interesse se materializa no desenvolvimento de tecnologias e algoritmos de modo a permitir a criação de sistemas de reconhecimento facial precisos e robustos. As vantagens desta tecnologia sobre outras modalidades biométricas a tornam uma aliada em potencial para segurança pública. Neste sentido, este texto busca analisar os impactos do emprego do reconhecimento facial na segurança pública no Brasil– considerando seus aspectos tecnológico e social – e discutir os potenciais mecanismos de controle jurídico, ético e social. O texto encerra indicando a necessidade de (a) criação de ambientes propícios às novas soluções tecnológicas, (b) o desenvolvimento tecnológico autóctone; (c) fortalecimento do arcabouço jurídico e normativo nacional; (d) adequação das instituições à legislação e normativas sobre proteção de dados; (e) pesquisas contínuas e maior atenção às fronteiras entre o uso de tecnologias de reconhecimento facial e a garantia de direitos; e (f) realização de estudo prospectivo para confrontar a realidade atual com as necessidades de adequações em âmbito nacional no uso do reconhecimento facial na segurança pública.

Palavras-chave: Segurança pública, reconhecimento facial, inteligência artificial, Brasil.

Resumen
El reconocimiento facial se emplea cotidianamente en nuestras vidas. Desde 1960, cuando se iniciaron investigaciones sobre el tema hasta hoy, creciendo este a un ritmo acelerado debido a que existe un interese en visibilizar el procesamiento automatizado de imágenes digitales para reconocimiento facial para una amplia gama de aplicaciones, por ejemplo, autenticación

biométrica, vigilancia, interacción computador-humano, entre otros. Ese interés se materializa en el desarrollo de tecnologías y algoritmos, de modo que, permite la creación de sistemas de reconocimiento facial precisos y robustos.

Las ventajas de esta tecnología sobre otras modalidades biométricas la convierten en una aliada potencial para la seguridad pública. En este sentido, este artículo busca analizar los impactos del empleo del reconocimiento facial en la seguridad pública en el Brasil –considerando sus aspectos tecnológico y social –y discutir los potenciales mecanismos de control jurídico, ético y social. El texto comprende la necesidad de: (a) la creación de ambientes propicios a las nuevas soluciones tecnológicas, (b) el desarrollo tecnológico propio, (c) fortalecimiento de la estructura jurídica y normativa nacional, (d) adecuación de las instituciones a la legislación y normativa sobre protección de datos, (e) investigaciones continuas y mayor atención a las fronteras entre el uso de tecnologías de reconocimiento facial y la garantía de derechos, y (f) realización de estudio prospectivo para confrontar la realidad actual con las necesidades de adecuaciones en el ámbito nacional en el uso de reconocimiento facial en la seguridad pública.

Palabras-clave: Seguridad pública, reconocimiento facial, inteligencia artificial, Brasil.

INTRODUÇÃO

Alguns clichês são frequentemente evocados ao se falar de vigilância e controle, dentre eles, a famosa sociedade distópica de Orwell, radicada na ideia do Big Brother, um modelo em que os cidadãos vivem sob vigilância constante por parte do Estado autoritário. Desde então, o romance passou a ser referência na cultura mainstream para se referir a iniciativas, sejam elas estatais ou não, que culminam na invasão de privacidade e violação de direitos.

O princípio explorado por Orwell em sua obra é fundado no ideal do panóptico, segundo o qual o sujeito "é visto, mas não vê; objeto de uma informação, nunca sujeito numa comunicação" (Foucault 2011, p. 224). Este princípio ganha especial pertinência com a ampliação do uso de inteligência artificial nas sociedades contemporâneas e com a pervasividade de geração e compartilhamento de dados pessoais facilitados pela popularização de artefatos tecnológicos e redes sociais[1].

Reconhecimento facial é uma habilidade empregada cotidianamente em nossas vidas. Desde 1960, quando se iniciaram as pesquisas, até hoje, em um ritmo crescentemente acelerado, há interesse em viabilizar o processamento automatizado de imagens digitais para reconhecimento facial para uma ampla gama de aplicações, tais como: autenticação biométrica vigilância, interação computador-humano, entre outros. Este interesse se materializa no desenvolvimento de tecnologias e algoritmos de modo a permitir a criação

1 Estendemos a compreensão de Susan Star acerca de infraestruturas em nossa leitura de sistemas de vigilância com reconhecimento facial. Neste sentido, a autora indica que as infraestruturas não são globais nem verticais, porquanto operam umas em relação às outras. Entendemos que o reconhecimento facial, é uma infraestrutura, já que se integra à diferentes infraestruturas como câmeras de segurança, smartphones, drones, entre outros (Star 1999).

de sistemas de reconhecimento facial precisos e robustos. As vantagens desta tecnologia sobre outras modalidades biométricas a tornam uma aliada em potencial para segurança pública.

Conforme o Fórum Brasileiro de Segurança Pública (FBSP), a segurança pública tem como premissa a prevenção e a repressão qualificada, sempre respeitando a dignidade humana, respeitando os Direitos Humanos e o Estado democrático de Direito. Trata-se, portanto, de um serviço público. Assim como o acesso à saúde, à educação e à moradia, a garantia de ir e vir com segurança é um direito fundamental previsto pela Constituição Federal de 1988 – CF/88, sendo dever do Estado assegurá-lo. O Art. 144 da CF/88 diz que a segurança pública, dever do Estado, direito e responsabilidade de todos, é exercida para a preservação da ordem pública e da segurança e proteção das pessoas e do patrimônio, através dos seguintes órgãos: Polícia federal; Polícia rodoviária federal; Polícia ferroviária federal; Polícias civis; Polícias militares e corpos de bombeiros militares (Faria 2018). Esses órgãos são os potenciais usuários da tecnologia de reconhecimento facial no âmbito da segurança pública.

Neste sentido, este texto busca analisar os impactos do emprego do reconhecimento facial na segurança pública no Brasil– considerando seus aspectos tecnológico e social – e discutir os potenciais mecanismos de controle jurídico, ético e social. Metodologicamente de natureza bibliográfica, o trabalho foi realizado consultando produções recentes na área. O texto se organiza em seções para abordar os aspectos tecnocientíficos do reconhecimento facial, seu emprego na segurança pública, os aspetos sociais no contexto brasileiro e finalmente, aborda os mecanismos de controle e as potencialidades de um estudo prospectivo no tema, sem deixar de considerar o período de pandemia provocado novo coronavírus (SARS-CoV-2).

Aspectos tecnológicos do reconhecimento facial

Dentre as aplicações mais celebradas da inteligência artificial, sobretudo do ponto de vista da vigilância, encontramos o reconhecimento facial. Habilidade empregada cotidianamente em nossas vidas, o reconhecimento facial é um traço cognitivo humano no qual se inspiram desenvolvedores na busca por viabilizar o processamento automatizado de imagens digitais. O reconhecimento facial é ainda visto como uma tecnologia promissora, este interesse se materializa no desenvolvimento de tecnologias e algoritmos de modo a permitir a criação de sistemas de reconhecimento facial precisos e robustos.

A robustez dos sistemas de reconhecimento facial é uma de suas características mais críticas e frequentemente uma das mais problemáticas, e diz respeito aos parâmetros que influenciam a performance do reconhecimento facial em ambientes não controlados, bem como desafios impostos pelo envelhecimento, visibilidade parcial e expressões faciais (Mou 2010). Por "ambiente não controlado" é referida como tradução livre de *unconstrained enviroments*, quer dizer, a captura de imagens em ambientes em que a imagem do sujeito é capturada em um contexto espontâneo — na rua, no transporte público, etc. —, o que leva a variações de ângulo, escala, oclusão, condições de luminosidade, interferência de fundo da imagem, entre outros.

O efeito negativo de parâmetros inadequados pode ser mitigado através da ampliação do banco de dados, cujo limite é crescentemente expandido pelo potencial emprego de big data, definido como conjuntos massivos de dados que precisam ser processados e armazenados. Assim, caso o banco de dados conte com registros fotográficos diferentes — como fotos de identificação, fotos de redes sociais —, e em ambientes variados e puder atualizá-los com registros mais recentes, as técnicas de reconhecimento produzem resultados significativamente robustos (Mou 2010). As vantagens desta tecnologia sobre outras modalidades biométricas[2] — a exemplo da invasividade nula, a tornam uma aliada em potencial para a vigilância e para a segurança pública.

Tais vantagens são decorrentes do desenvolvimento e aprimoramento pelos quais vem passando a inteligência artificial. Definida como estudo de dispositivos e sistemas computacionais construídos para agir de uma maneira que estaríamos inclinados a compreender como sendo inteligentes (Berkeley [s.d.]), a inteligência artificial é um vasto e profícuo campo do conhecimento. Sua evolução aponta para os processos de *machine learning* ou aprendizado automático.

Enquanto a inteligência artificial inclui raciocínios dedutivos e indutivos, o *machine learning* se detém no modelo indutivo e se baseia em algoritmos que operam construindo modelos com base em inputs amostrais para fazer previsões ou decisões orientadas pelos dados e não por instruções previamente programadas (Kohavi e Provost 1998). O aprendizado automático, representa, portanto, a habilidade de máquinas aprenderem sem serem explicitamente programadas (Simon 2013), fazendo previsões a partir de dados e aperfeiçoando o próprio funcionamento considerando seus erros (Kohavi e Provost 1998).

A complexificação do aprendizado de máquina conta com vários ramos, dentre os quais, o aprendizado profundo, ou *deep learning*. Esta modalidade é projetada de modo a mimetizar características neurais humanas. É frequente que se associe o *deep learning* com o cérebro humano em muitas das divulgações da mídia sobre o tema. Entretanto, pesquisadores do campo frequentemente baseiam mais em áreas como álgebra linear, probabilidade, teoria da informação, entre outros, permanecendo o cérebro humano apenas como uma influência e não como algo a ser simulado. Uma das razões para isto é o fato de que não dispomos de informação o suficiente sobre o cérebro humano para guiar os desenvolvimentos em *machine learning* em geral (Goodfellow, Bengio, e Courville 2016).

Com auxílio da estatística e matemática aplicada, graças a computadores com maior capacidade de processamento para trabalhar com conjuntos de dados maiores e dotados de técnicas para treinar redes mais profundas (Goodfellow et al. 2016), o *deep learning* representa um salto para a inteligência artificial, uma vez dispensa a inserção manual de parâmetros de leitura e processamento de imagens com a finalidade de extrair as características

2 Biometria é a ciência de reconhecer a identidade de uma pessoa com base em características físicas ou comportamentais. As tecnologias disponíveis para a biometria incluem: impressões digitais, face, voz, íris, veias das mãos, forma de caminhar, e vincos (Jain, Flynn, e Ross 2008).

faciais mais importantes. Com este implemento, o desenvolvedor treina a máquina, e as conexões e ilações por ela realizadas na consecução da tarefa de processamento e aprendizado se tornam uma caixa preta[3].

Do ponto de vista técnico, pode-se resumir as etapas do algoritmo de aprendizado de máquina como: encontrar um rosto na imagem, focar um rosto por vez, compreender os diferentes ângulos e iluminações sob os quais um mesmo rosto pode se apresentar; identificar características únicas no rosto humano que permitam distinguir entre rostos diversos; e, por fim, comparar as características distintivas de um rosto com os rostos constantes no banco de dados e encontrar o nome da pessoa a quem o rosto pertence.

O resultado do emprego de *deep learning* para reconhecimento facial é o aprimoramento da precisão de previsões e identificações, que atualmente vêm sendo empregada de forma consistente e bem sucedida em aplicações diversas nos setores público e privado, se apresentando como a única abordagem que constrói sistemas de inteligência artificial capazes de operar em ambientes reais complexos, a exemplo de carros autônomos, nos quais a tomada de decisão e reconhecimento dos objetos encontrados comumente na trajetória de um carro nas ruas é complexo, e imagens de vídeo capturadas em sistemas de monitoramento segurança.

Atualmente, algumas ferramentas de busca já incorporaram o *deep learning* para reconhecimento facial em vários contextos, inclusive para uso público, a exemplo da plataforma de busca russa Yandex (Mazumdar 2020). Nela, o mecanismo de busca de imagens reversa — aquele em que se busca por outras imagens/fotos semelhantes — conta com o reconhecimento facial. Como resultado, a plataforma permite ter, como resultado da busca, não simplesmente fotos parecidas com aquela introduzida, mas sim o nome da pessoa retratada na foto ou outras fotos da mesma pessoa.

O reconhecimento facial é mais uma das tecnologias que passaram a fazer parte da rotina das pessoas durante a pandemia de Covid-19. A partir do momento em que foi preciso repensar a interação social a partir da perspectiva da limitação do contato e criar estratégias de proteção e preservação da saúde, a tecnologia envolvida em um sistema de reconhecimento facial mostrou-se ainda mais eficiente. Em alguns momentos, como na captação de imagens dos passageiros em aeroportos, ou metrôs, ou mesmo na coleta de dados pessoais de pacientes, é sempre presente o risco de perdas de direitos fundamentais à privacidade.

O ano de 2020 está marcado como o ano em que a Terra precisou parar e se reinventar. E, como é típico em momentos de crises, a forma como cada nação está lidando com a pandemia de Covid-19 diz muito sobre sua história, seus dirigentes, suas instituições e sobre o seu patamar civilizatório (Fórum Brasileiro de Segurança Pública 2020, p.14).

3 Cientistas estão pesquisando para melhorar este aspecto, entretanto, o deep learning continua sendo uma das técnicas a serem usadas no machine learning e no reconhecimento facial. De um ponto de vista técnico, é importante notar que a aplicação de reconhecimento facial tem várias tarefas para detectar imagens, por exemplo, classificação, localização e detecção de objetos (Li, Johnson, e Yeung 2017b). Deve-se notar que o reconhecimento facial não utiliza a segmentação de objetos, pois sua finalidade é a detenção do rosto humano.

A história nesse período de pandemia está acontecendo de forma muito acelerada. Vários futuristas internacionais dizem que o coronavírus funciona como um acelerador de futuro (Melo 2020) e "fala-se da antecipação de aproximadamente cinco anos no curso da história" (Costa 2020, p.18)

Reconhecimento facial na segurança pública

No setor público a aplicação na área de segurança pública é uma realidade. 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. Pesquisas estimam que metade dos adultos dos Estados Unidos estão registrados em bancos de dados da polícia norte americana, o que representa 117 milhões de cidadãos cujos dados se encontram à disposição para rastreamento pelas autoridades (Garvie, Bedoya, e Frankle 2016).

A robustez dos sistemas, apesar de apresentar taxas cada vez melhores de eficácia no reconhecimento facial baseado em banco de dados públicos e privados, não atinge números absolutos. Recentemente, estudos desenvolvidos pelo Instituto Nacional de Padronização e Tecnologia dos Estados Unidos, chegaram à conclusão de que algoritmos de reconhecimento facial apresentam viés para identificação de pessoas negras e asiáticas, especialmente mulheres (Grother, Ngan, e Hanaoka 2019). Este viés se dá em função da composição do banco de dado no qual se baseia o aprendizado de máquina ser mais abrangente para homens brancos do que para grupos étnicos minoritários. Esta questão torna a aplicação da tecnologia ainda mais controversa.

Tais ferramentas podem ser empregadas por empresas privadas que têm governos como clientes para aplicações em seus sistemas de segurança pública. Por um lado, esta tecnologia pode ser aliada ao combate à criminalidade, enquanto, por outro, representa uma ampla mudança em nossas vidas não apenas virtuais — em função da exposição a qual nos submetemos voluntariamente em nossas vidas cotidianas através das redes sociais —, mas também em nossas vidas reais, haja vista que reduz o controle sobre a privacidade individual e vai de encontro ao direito ao anonimato público, acarretando invasão de privacidade em nossas vidas cotidianas. Para o bem ou para o mal, espaços públicos são convertidos em territórios de vigilância.

Exemplos de experiências recentes põem à prova a dupla natureza deste tipo de tecnologia e os perigos de seu emprego. Nos Estados Unidos, onde uma ONG chamada *Thorn* já ajudou a identificar mais de 10 mil vítimas de tráfico sexual de crianças e as resgatar de situações de divulgação de pornografia infantil[4]. Em Hong Kong, sob um governo de tendência autoritária, a tecnologia foi usada para constranger indivíduos, tolher a liberdade de expressão e impor condutas, quando dos protestos pró-democracia, que tiveram lugar ao

4 Dados fornecidos pelo relatório de 2018 no site da ONG Thorn, https://www.thorn.org/impact-report-2018/. Acesso em 17/05/2020.

longo de 22 semanas em 2019. Na ocasião, autoridades usaram programas de reconhecimento facial para identificar e inibir manifestantes, muitos dos quais acabaram por ser presos.

Mesmo os gigantes da tecnologia defendem a regulação destas tecnologias. Dentre eles, a empresa Google, cujo slogan já foi *AI First*, em tradução livre, Inteligência Artificial em primeiro lugar. Em pronunciamento[5] a empresa afirmou que a prioridade da empresa no momento é fazer com a que a inteligência artificial beneficie o maior número de pessoas e reconheceu que chegou a hora de regulamentar a abordagem de aplicação da tecnologia. A ideia é que a regulamentação forneça orientações amplas, viabilizando uma implementação personalizada para diferentes setores, com regras apropriadas que considerem custos e benefícios relevantes. Por exemplo, para a implementação de c**ontrole de acesso e ponto com reconhecimento facial e análise de temperatura e máscaras**[6]**.**

Aspectos sociais do reconhecimento facial no contexto brasileiro

A compreensão dos meandros técnicos envolvidos na tecnologia do reconhecimento facial é importante sobretudo para perceber adequadamente seus aspectos positivos e negativos. A não-manipulação direta pelo usuário mitiga as possibilidades tanto de vandalismo quanto de falsidade ideológica em aplicações que usam o reconhecimento facial, já que não há necessidade de memorização de senhas, ou códigos de identificação. Em contrapartida, o fato de que os sistemas até hoje desenvolvidos não conseguirem atingir taxas absolutas de precisão, sobretudo com imagens captadas em ambientes não controlados e a presença de vieses nos algoritmos de processamento, representam uma dificuldade objetiva ao uso ampliado do reconhecimento facial na segurança pública.

Debates éticos, jurídicos e sociais já presentes em países do norte global se intensificam em outras localidades, sobretudo no cenário nacional, a partir da adoção de sistemas de monitoramento com reconhecimento facial em cidades brasileiras. É o caso de ao menos 37 cidades, segundo a Agência Brasil. Dados do Instituto Igarapé (2019) demonstram que a tecnologia vem sendo utilizada desde 2011, tendo ganhado especial visibilidade em 2019. No Brasil, a principal aplicação é feita na área de transporte público, com vistas a identificar fraudes no uso de benefícios de gratuidade. Porém, observa-se a expansão de seu emprego na segurança pública.

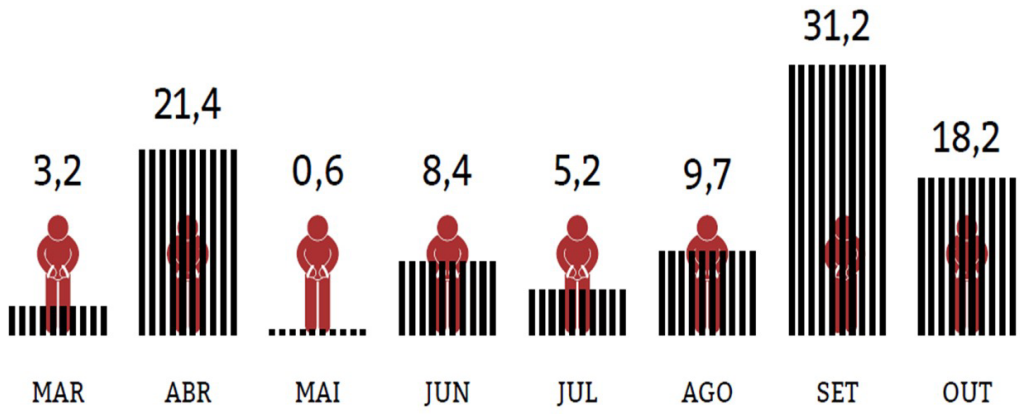
No início deste 2020, o Governo de São Paulo inaugurou um laboratório de reconhecimento facial e digital da Polícia Civil. Nele, as imagens obtidas são analisadas à luz dos dados biométricos coletados durante a emissão do Registro Geral – RG, e então submetidos ao Sistema de Identificação Automatizada de Impressões Digitais – *Automated Fingerprint Identification System*, para confirmação da identidade do requerente (Governo de São Paulo 2020).

5 https://www.zdnet.com/article/google-io-from-ai-first-to-ai-working-for-everyone/ (Condon 2019).

6 Usa-se uma espécie de totem com leitor térmico facial tornando-se numa importante ferramenta de controle e gestão. A leitura facial evita contatos, a inteligência artificial embarcada traz análise de temperatura do usuário e análise de uso de mascará. Podendo ser utilizada em locais com grande fluxo de pessoas, auxiliando não só no controle de acesso, bem como na gestão de dados para compreender a disseminação do novo coronavírus.

O cruzamento destes dados com imagens captadas em locais de crime e fragmentos de impressões digitais são enviadas para uma equipe especializada, que submeterá o material à análise com emprego da nova tecnologia, alegadamente diminuindo as margens de erro para identificação de suspeitos. A tecnologia, considerando potenciais falhas que pode apresentar, não é utilizada isoladamente como meio de prova, mas sim, atrelada a outros procedimentos da Polícia Civil Estadual no contexto de uma investigação criminal. Esta expansão do uso de reconhecimento facial no contexto da segurança pública no Brasil requer um debate qualificado, considerando não apenas os benefícios, mas também os riscos envolvidos (Nunes 2019).

Figura 1. Proporção de prisões efetuadas com uso de reconhecimento facial



Rede de Observatório da Segurança (Nunes 2019)

A convergência entre uma crescente disponibilidade de imagens faciais digitais, a ampliação de seu emprego na esfera pública e taxas de erro cada vez menores em mecanismos de reconhecimento facial são os pontos de partida para o presente texto. O problema, assim posto, remete a questões técnicas, éticas, jurídicas e sociais levantadas a partir da incorporação da tecnologia de reconhecimento facial na segurança pública no contexto nacional. Neste sentido, nosso objetivo principal é conhecer do uso do reconhecimento facial na segurança pública no Brasil.

Além do já abordado aspecto tecnológico e científico do reconhecimento facial, podemos contextualizar alguns aspectos sociais. Estudos recentes do Instituto Nacional de Padrões e Tecnologia Norte Americano, o NIST, constataram a existência do que chamaram de diferenciais, ou seja, a capacidade de um algoritmo de corresponder a duas imagens da mesma pessoa varia de um grupo demográfico para outro. Naturalmente a análise do viés e em que proporção este se apresenta não pode ser feita para todos algoritmos. Cada um apresenta diferenciais distintos (National Institute of Standards and Technology 2019).

Há uma notória preocupação entre cientistas sociais e juristas considerando que o emprego do reconhecimento facial possa reforçar a seletividade do sistema penal brasileiro (Da Silva e Da Silva 2019), uma vez que há vieses quanto a etnia e gênero que podem comprometer ainda mais a confiabilidade dos resultados obtidos através do emprego da tecnologia. A forma de funcionamento do *deep learning* dificulta a eliminação de tais vieses, uma vez que não é explícito o funcionamento das redes neurais desenvolvidas por *machine learning*.

Em seus mais de 300 anos de escravidão, pode-se observar que o racismo estrutural da sociedade brasileira se projeta no uso da ferramenta. Um teste realizado no carnaval do Rio de Janeiro em 2019 indicou um índice de erro de 90% nas detenções da polícia local com base no uso e identificação por reconhecimento facial. Essa e outras pesquisas mostram que homens brancos são reconhecidos com mais assertividade pela tecnologia do que mulheres negras (Taute 2020). As razões para essa discrepância passam pela já citada necessidade de aprimoramento da tecnologia e vão de encontro às questões sociais que envolvem o aparato tecnológico. Da Silva e Da Silva (2019) observaram que os entraves para o desenvolvimento mais acurado deste tipo de tecnologia não prescindem da formação e emprego de quadros técnicos mais diversos nas empresas desenvolvedoras.

O reconhecimento facial fornece, muitas vezes sem autorização prévia, uma enorme quantidade de dados e informações pessoais que podem ser utilizados tendo lícitos como principal finalidade. Conforme Pinheiro (2020), a informação é um dos ativos mais valiosos de que dispomos, e a proteção de dados, prioridade absoluta. No campo dos mecanismos de controle ético, percebe-se que a amplitude de possibilidades de uso da inteligência artificial cria novos nichos de mercado, altamente rentáveis, como é o caso da segurança pública, nosso foco. Porém ainda não há muitas garantias quanto ao emprego de forma ética e responsável, tanto por parte de governos como de empresas.

Com medo de espalhar o coronavírus, as empresas de segurança estão argumentando que os sistemas de reconhecimento facial podem ser uma opção mais segura e mais limpa do que os sistemas biométricos tradicionais para controle de acesso. Serve para detectar se alguém está com febre e solicitar que a pessoa deixe uma instalação ou procure atendimento médico. A alegação não vem sem controvérsia, pois os scanners de impressões digitais se tornaram cada vez mais comuns como soluções de controle de acesso[7] e o armazenamento dos dados coletados podem, conforme já explicitado, serem gerenciados de forma não tão idônea.

A falta de normatização e regulação adequada pode favorecer que os dados pessoais sejam também usados ilegalmente, donde a necessidade de mecanismos de controle, amplamente debatidos, com participação da sociedade civil organizada, que garantam à sociedade a observação de tais aspectos éticos e legais (De Oliveira 2020).

7 Fonte: https://revistasegurancaeletronica.com.br/os-sistemas-de-reconhecimento-facial-podem-aumentar-em-popularidade-durante-a-pandemia-de-coronavirus/ (Segurança eletrônica [s.d.])

Mecanismos de controle e a importância da realização de estudos prospectivos

Quanto aos mecanismos de controle jurídico, internacionalmente o debate se encontra mais avançado, sobretudo nos países do norte global, o que se expressa por meio da promulgação de legislações com vistas a aprimorar a governança dos dados pessoais pelas empresas, órgãos públicos e demais instituições, reunindo as boas melhores práticas. Um dos principais exemplos é o *General Data Protection Regulation*, resolução em vigor desde 25 de maio de 2018, na União Europeia, e propulsora da criação da recém aprovada Lei Geral de Proteção de Dados (LGPD) no Brasil (Pinheiro 2020).

A LGPD, vigente desde 18 de setembro de 2020, tem objetivo de garantir transparência no tratamento de dados pessoais da pessoa natural em qualquer meio. Ela prevê sanções que vão desde uma advertência até uma multa. No entanto, as punições só devem ser aplicadas a partir de agosto de 2021 e ficará a cargo da Autoridade Nacional de Proteção de Dados (ANPD). Em suma, concede ao cidadão o direito à propriedade sobre seus dados pessoais, e restringe o uso de tais dados por parte de organizações, condicionando-o ao cumprimento de regras de permissão (Fontes 2020). Apesar de a LGDP não se aplicar diretamente à segurança pública, ela traz alguns mecanismos para que as autoridades de segurança se atentem à questão da proteção de dados[8], podendo deflagrar maior coordenação dos entes federados que até então regulam somente sistemas já em operação.

Confirmam a preocupação sobre o caráter ético do emprego desta tecnologia o fato de que bases de dados públicas e privadas – algumas contendo informações detalhadas sobre as vidas civil e penal das pessoas – já coletavam registros faciais e biométricos mesmo antes do país aprovar a sua lei de proteção de dados pessoais (Instituto Igarapé 2019).

Regular o emprego de qualquer tecnologia emergente é complexo, uma vez que a linha que separa a necessária preservação de direitos civis e o usufruto das transformações proporcionadas pela inovação tecnológica é tênue, sobretudo considerando que a avaliação de tecnologias muitas vezes só é viável à posteriori. O uso de tecnologias emergentes por parte do setor público representa, nesse cenário, um desafio ainda maior, uma vez que se trata de instituições diretamente responsáveis pela preservação do interesse da sociedade (Francisco, Hurel, e Rielli 2020).

Com o objetivo de tratar estratégias de combate à pandemia, dados pessoais são coletados para serem administrados em prol de um bem coletivo maior - evitar contaminação e/ou garantir ambientes mais seguros, sem consentimento prévio das pessoas e sem conhecimento sobre as regras de segurança no uso dos dados. No âmbito da LGPD da Presidência da República do Brasil (2018), trata-se de dados sensíveis. O tratamento, sem o consentimento do titular é exceção, podendo ocorrer somente nas hipóteses previstas na própria LGPD (art. 11, II). Ou seja, é uma boa prática sempre obter o prévio consentimento das pessoas para coleta, armazenamento e uso de seus dados sensíveis.

8 Informação em Dadocracia podcast (Dataprivacy Br 2020).

A preocupação em tratar dignamente, ou com o mínimo de segurança possível, não tem sido debatido e caracterizado ampla e corretamente. Ao contrário, "governos, de forma ardilosa, tentam aproveitar o caos pandêmico para impingir a seus cidadãos retrocessos em seus direitos fundamentais (Costa 2020, p.18). Consequentemente, infere-se que as tecnologias de coleta de dados, além do viés já citado, não estão adequadamente estruturadas/preparadas garantir e evitar o uso indevido das informações dos cidadãos ali armazenadas.

A maior parte das análises feitas até aqui se beneficiaria da realização de um estudo prospectivo – *foresight*. Para Miles, *foresight* é o termo usado para descrever o estudo sistemático do futuro – especialmente de um futuro transformado pelo uso de novas tecnologias (Miles 2008). Uma das funções da abordagem prospectiva no desenvolvimento de políticas de pesquisa e inovação é justamente o da correção, na qual as deficiências e falhas sistêmicas são identificadas e formalizadas pelos participantes da prospecção (Georghiou e Harper 2011).

A prospecção permitiria identificar a magnitude dos impactos do uso do reconhecimento facial na segurança pública e subsidiar a priorização de ações para a implementação de uma política de pesquisa e inovação em nível nacional, que garantisse um modelo de participação social (Cruz-Castro e Sanz-Menéndez 2005), envolvendo especialistas juntamente com a sociedade.

Afirma-se que as melhores metodologias prospectivas são aquelas que combinam técnicas com abordagens quantitativa e qualitativa, conquistando as ideias que vêm de cada uma. Então, para uma ampla e completa execução desse estudo, sugere-se o uso de métodos de prospecção quantitativos, baseados em (1) benchmarking e (2) análise de dados de empresas que já atuam na temática; e o uso de métodos de prospecção qualitativos, que utilizarão a opinião de especialista em novos negócios tecnológicos, através de (1) brainstormings, (2) *surveys*, (3) cenários, (4) painéis de especialistas e cidadãos (Popper 2008).

Assim, a etapa inicial constitui a identificação do patrocinador e do grupo de coordenação do estudo a partir do grupo de atores envolvidos. Os atores envolvidos seriam representados por grandes empresas de inteligência artificial, startups, institutos de pesquisa públicos e privados, universidades, consultorias, fornecedores, atores políticos (estadual e federal), gestores públicos da área de segurança pública, e representantes da sociedade civil organizada.

A representação social permitiria debater a aceitabilidade pública dos impactos desta tecnologia e legitimaria a tomada de decisão sobre políticas científicas e tecnológicas. Tratam a prospecção como fundamental para implantação política de ciência para inovação, uma vez que é um instrumento de articulação e de estruturação da política de forma colaborativa, pois alcança consenso e comprometimento entre os partícipes (Georghiou e Harper 2011).

Considerações finais

o emprego do reconhecimento facial na segurança pública é uma realidade. Neste contexto, ponderamos que:

- (a) ambientes propícios às novas soluções tecnológicas precisam ser criados para garantir que os atores do sistema de inovação participem de sua estruturação, em consonância com a Organização de Cooperação e de Desenvolvimento Económicos que alerta para a necessidade da criação de políticas ligadas ao desenvolvimento e difusão de tecnologia com base na inteligência artificial (OECD 2018). Inclui desde regulamentos que regem a privacidade de dados, regras de responsabilidade, de apoio à pesquisa e de propriedade intelectual.
- (b) o desenvolvimento tecnológico autóctone, adequados à cultura do país, poderia mitigar falhas oriundas de vieses nos algoritmos empregados. Entretanto, no contexto nacional, as partes interessadas, como por exemplo o setor produtivo e institutos de pesquisa, estão desprovidos de arcabouço de política científica que lhes auxilie a melhorar o investimento em pesquisa e desenvolvimento nesta área;
- (c) o arcabouço jurídico e normativo nacional precisa ser fortalecido para que a adoção do reconhecimento facial no sistema de segurança pública não reforce a seletividade do sistema penal brasileiro;
- (d) as instituições públicas ou privadas que trabalham com tratamento dos cidadãos brasileiros feita em território nacional, sediadas ou não no Brasil, terão que se adequar à LGPD com maior brevidade.
- (e) são necessárias pesquisas contínuas e maior atenção às fronteiras entre o uso de tecnologias de reconhecimento facial e a garantia de direitos são necessárias como forma de consubstanciar mais mecanismos de controle social, ético e jurídico no âmbito nacional;
- (f) um estudo prospectivo seria capaz de confrontar a realidade atual com as necessidades de mudanças para (o melhor) uso do reconhecimento facial como importante ferramenta na área de segurança pública sem deixar de considerar a preservação das informações/dados pessoais da população alvo e o auxílio às instituições e seus agentes responsáveis pela segurança pública no país.

Por fim, o uso de reconhecimento facial na segurança pública apresenta uma possibilidade extraordinária de melhoria na infraestrutura de segurança pública, entretanto, conforme apontado ao longo do texto, o emprego desta tecnologia, sobretudo no ramo discutido e num contexto de pandemia da Covid-19, não prescinde da constrição por mecanismos de controle ético, social e jurídico. No Brasil, as políticas que regulam o uso de tecnologia de

inteligência artificial, especificamente o de reconhecimento facial, têm se mostrado insuficientes no atendimento às necessidades e expectativas das partes interessadas, principalmente da sociedade.

Referências bibliográficas

berkeley, István. [s.d.]. "What Is Artificial Intelligence?" Recuperado 17 de maio de 2020 (https://userweb.ucs.louisiana.edu/~isb9112/dept/phil341/wisai/WhatisAI.html).

Condon, Stephanie. 2019. "Google I/O: From 'AI First' to AI Working for Everyone". *Zdnet*. Recuperado 17 de maio de 2020 (https://www.zdnet.com/article/google-io-from-ai-first-to-ai-working-for-everyone/).

Costa, Antônio Célio. 2020. "Privacidade e covid - 19: proteção do corpo eletrônico da pessoa, sob a ótica de Stefano Rodotà". *Revista Brasileira de Direitos e Garantias Fundamentais* 6(2):75–96. doi: 10.26668/IndexLawJournals/2526-0111/2020.v6i2.7164.

Cruz-Castro, Laura, e Luis Sanz-Menéndez. 2005. "Politics and Institutions: European Parliamentary Technology Assessment". *Technological Forecasting and Social Change* 72(4):429–48. doi: 10.1016/j.techfore.2004.01.007.

Da Silva, Rosane, e Fernanda Da Silva. 2019. "Reconhecimento Facial e segurança pública: os perigos do uso da tecnologia no sistema penal seletivo brasileiro". in *5 Congresso Internacional de Direito e Contemporaneidade: mídias e direitos da sociedade em rede*. Universidade Federal de Santa Maria.

Dataprivacy Br. 2020. *De olho em você*. Vol. Episódio 15.

De Oliveira, Gabriel Prado Souza. 2020. "Sigilo de Dados no Brasil: da Previsão Constitucional à Nova Lei Geral De Proteção De Dados Pessoais". *Revista Âmbito Jurídico*, fevereiro.

Faria, Ícaro. 2018. "Segurança pública brasileira: responsáveis, números e desafios". *Politize*. Recuperado 20 de julho de 2020 (https://www.politize.com.br/seguranca-publica-brasileira-entenda/).

Fontes, Edison. 2020. "O que você precisa saber sobre a Lei Geral de Proteção de Dados Pessoais". maio, 42–45.

Fórum Brasileiro de Segurança Pública. 2020. "Anuário Brasileiro de Segurança Público 2020".

Foucault, Michel. 2011. *Vigiar e punir: nascimento da prisão*. Petropolis: Vozes.

Francisco, Pedro Augusto, Louise Marie Hurel, e Mariana Marques Rielli. 2020. "Regulação do reconhecimento facial no setor público: avaliação de experiências internacionais".

Garvie, Clare, Alvaro Bedoya, e Jonathan Frankle. 2016. "The Perpetual Line-up: Unregulated Police Face Recognition in America". *Perpetua-*

llineup. Recuperado 17 de maio de 2020 (https://www.perpetuallineup.org/).

Georghiou, Luke, e Jennifer Harper. 2011. "From Priority-Setting to Articulation of Demand: Foresight for Research and Innovation Policy and Strategy". *Futures* 43(3):243–51. doi: 10.1016/j.futures.2010.11.003.

Goodfellow, Ian, Yoshua Bengio, e Aaron Courville. 2016. *Deep learning*. Cambridge, Massachusetts: The MIT Press.

Governo de São Paulo. 2020. "Governo inaugura laboratório de reconhecimento facial e digital da Polícia Civil". *São Paulo*. Recuperado 6 de agosto de 2020 (https://www.saopaulo.sp.gov.br/spnoticias/governo-inaugura-laboratorio-de-reconhecimento-facial-e-digital-da-policia-civil/).

Grother, Patrick, Mei Ngan, e Kayee Hanaoka. 2019. *Face Recognition Vendor Test (FRVT) part 2 :: identification*. NIST IR 8271. Gaithersburg, MD: National Institute of Standards and Technology.

Instituto Igarapé. 2019. "Reconhecimento facial no Brasil". *Instituto Igarapé*. Recuperado 17 de maio de 2020 (https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/).

Jain, Anil K., Patrick Flynn, e Arun A. Ross, orgs. 2008. *Handbook of Biometrics*. New York: Springer.

Kohavi, Ron, e Foster Provost. 1998. "Glossary of terms. Machine Learning—Special Issue on Applications of Machine Learning and the Knowledge Discovery Process". *Machine Learning* 30(2/3):271–74. doi: 10.1023/A:1017181826899.

Li, Fei-Fei, Justin Johnson, e Serena Yeung. 2017a."CS231n, Lecture 3: Loss Functions and Optimization". Apresentado em Convolutional Neural Networks for Visual Recognition, Stanford University.

Li, Fei-Fei, Justin Johnson, e Serena Yeung. 2017b."Lecture 2 | Image Classification". Apresentado em Convolutional Neural Networks for Visual Recognition, Stanford University.

Mazumdar, Tarun. 2020. "Russia's Yandex Is 'Creepy': Its Search Engine Uses Facial Recognition To Expose Identities In Anonymous Images". *International Business Times*. Recuperado 17 de maio de 2020 (https://www.ibtimes.com/russias-yandex-creepy-its-search-engine-uses-facial-recognition-expose-identities-2904470).

Melo, Clayton. 2020. "Como o coronavírus vai mudar nossas vidas: dez tendências para o mundo pós-pandemia". *El País*.

Miles, Ian, org. 2008. "From Futures to Foresight". in *The handbook of technology foresight: concepts and practice*, *Prime series on research and innovation policy*. Cheltenham, UK. Northampton, Mass: Edward Elgar.

Mou, Dengpan. 2010. *Machine-Based Intelligent Face Recognition*. Beijing: Higher Education Press.

National Institute of Standards and Technology. 2019. "NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software". *National*

Institute of Standards and Technology. Recuperado 6 de julho de 2020 (https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software).

Nunes, Pablo. 2019. "Novas ferramentas, velhas práticas: reconhecimento facial e policiamento no Brasil". *Retratos da violência cinco meses de monitoramento, análises e descobertas*, 67–71.

OECD. 2018. "Artificial Intelligence and the Technologies of the Next Production Revolution". in *OECD Science, Technology and Innovation Outlook 2018: Adapting to Technological and Societal Disruption*, *OECD Science, Technology and Innovation Outlook*. OECD.

Pinheiro, Peck. 2020. "Qual o impacto da LGPD em instituições de ensino e pesquisa? Rede Nacional de Pesquisa e Ensino (RNP)". *Rede Nacional de Ensino e Pesquisa*. Recuperado 6 de junho de 2020 (https://www.rnp.br/noticias/qual-o-impacto-da-lgpd-em-instituicoes-de-ensino-e-pesquisa).

Popper, Rafael. 2008. "Foresight Methodology". in *The handbook of technology foresight: concepts and practice*, *Prime series on research and innovation policy*. Cheltenham: Elgar.

Presidência da República do Brasil. 2018. *Lei Nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD)*.

Segurança eletrônica. [s.d.]. "Os sistemas de reconhecimento facial podem aumentar em popularidade durante a pandemia de coronavírus". *Segurança eletrônica*. Recuperado 20 de fevereiro de 2021 (https://revistasegurancaeletronica.com.br/os-sistemas-de-reconhecimento-facial-podem-aumentar-em-popularidade-durante-a-pandemia-de-coronavirus/).

Simon, Phil. 2013. *Too big to ignore: the business case for big data*. Hoboken, New Jersey: John Wiley & Sons, Inc.

Star, Susan Leigh. 1999. "The Ethnography of Infrastructure". *American Behavioral Scientist* 43(3):377–91. doi: 10.1177/00027649921955326.

Taute, Fabian. 2020. "Reconhecimento Facial e suas controvérsias". *Heinrich Boll Stiftung*. Recuperado 26 de junho de 2020 (https://br.boell.org/pt-br/2020/02/05/reconhecimento-facial-e-suas-controversias).