Revista Tecnologia e Sociedade
ISSN: 1984-3526

https://periodicos.utfpr.edu.br/rts

Aspectos ético-jurídicos e técnicos do emprego de reconhecimento facial na segurança pública no Brasil

Loryne Viana de Oliveira
loryne@ymail.com
Departamento de Política Científica e Tecnológica, Unicamp, Campinas, São Paulo.

Margarete Esteves Nunes Crippa
margarete.crippa@gmail.com
Departamento de Política Científica e Tecnológica, Unicamp, Campinas, São Paulo.

Ítala Laurente
Itala.laurente@gmail.com
Departamento de Política Científica e Tecnológica, Unicamp, Campinas, São Paulo.

Tamires Holanda
tami.holanda@gmail.com
Laboratório de Estudos Avançados em Jornalismo, Unicamp, Campinas, São Paulo.

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, utilizado em uma ampla gama de aplicações dentre as quais a vigilância e segurança pública. A presente pesquisa, de caráter bibliográfico-documental, busca analisar os impactos do emprego do reconhecimento facial na segurança pública no Brasil– considerando seus aspectos ético, jurídico, técnico e social, com o intuito de discutir os atuais e potenciais mecanismos de controle. A conclusão indica a necessidade de realização de debates mais amplos, em que, além do técnico, variados aspectos sejam avaliados em prol de uma discussão qualificada do emprego da tecnologia, sobretudo considerando a atual expansão de seu uso por autoridades públicas em todo país na esfera estadual.

PALAVRAS-CHAVE: Segurança Pública no Brasil. Reconhecimento Facial. Vigilância. Inteligência Artificial.

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). Neste contexto, o princípio do panóptico, apresentado inicialmente por Jeremy Bentham em 1785 e reapresentado por Foucault (2011; 2014), ganha um paralelo contemporâneo no conceito de Pasquale (2015) de *one-way mirror*: agentes públicos e privados passam a acumular toda sorte de dados de indivíduos, enquanto estes nada sabem daqueles.

A ampliação do uso de inteligência artificial nas sociedades contemporâneas, a ubiquidade de aparatos tecnológicos informacionais, e a popularização do acesso à geração e compartilhamento de dados pessoais – facilitados pela difusão destes artefatos e adesão massiva às redes sociais – são elementos chave para compreender os processos econômicos e políticos contemporâneos. Dados pessoais se tornam o centro da *data-driven economy*, tamanha a relevância por eles assumida no contexto atual do capitalismo (SRNICEK, 2018). Este novo padrão de produção e uso de dados pessoais, além de modificar as divisas entre sociedade e objetos técnicos, reconfigura práticas e instrumentos de vigilância, conferindo métodos diversos à disposição do Estado e empresas privadas para exercício da vigilância[1] (PERON; ALVARÉZ; CAMPELLO, 2018).

No campo da vigilância, o reconhecimento facial é uma tecnologia emergente central. 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 em uma ampla gama de aplicações, dos quais autenticação biométrica, vigilância, interação computador-humano, são apenas alguns exemplos. Este interesse se materializa no desenvolvimento de artefatos tecnológicos 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 um alvo preferencial para emprego na vigilância e segurança pública[2].

Consoante o Fórum Brasileiro de Segurança Pública (FBSP), a segurança pública tem como premissa a prevenção e repressão qualificada, sempre respeitando a dignidade humana, 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, que no artigo 144, a trata como sendo dever do Estado, direito e responsabilidade de todos, sendo 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.

A incorporação da tecnologia de reconhecimento facial suscita debates importantes, opondo seus benefícios e riscos. "Efervescente arena regulatória"

domina o cenário nacional enquanto o país registra atualmente a tramitação de três projetos de lei com o fito de regulamentar o emprego do reconhecimento facial (FRANCISCO; HIUREL; RIELLI, 2020).

Frente ao exposto, formulamos como objetivo geral desta investigação analisar os impactos do emprego de reconhecimento facial na segurança pública brasileira. De enfoque qualitativo e natureza bibliográfica, a pesquisa obedeceu a um processo indutivo, conformado por exploração, descrição e discussão de perspectivas teóricas. A definição do enfoque qualitativo se seu em função do objeto complexo de nossa investigação, além da almejada interdisciplinaridade ao conjugar aspectos jurídicos, sociais e técnicos para abordar o tema. Foi realizada uma análise documental, considerando fontes de pesquisas semelhantes entre Brasil e Europa no contexto da Lei Geral de Proteção de Dados (LGPD), Lei n° 13.709 de agosto de 2018, e o Regulamento Geral para a Proteção de Dados europeu (RGPD), bem como o anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal (LGPD-penal), elaborado no âmbito da Câmara dos Deputados do Brasil. Fontes não acadêmicas (documentos oficiais de governos e de centros de pesquisa independentes, textos para discussão de agências e órgãos públicos nacionais e internacionais) foram importantes à medida que a discussão enseja desdobramentos mais céleres do que os que usualmente são retratados em fontes estritamente acadêmicas. O texto se organiza em seções para abordar os aspectos tecnocientíficos do reconhecimento facial, seu emprego na segurança pública, os aspectos sociais no contexto brasileiro e, finalmente, análise da LGPD, e os mecanismos de controle e jurídico, ético e social existentes.

ASPECTOS TECNICOS 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. As tecnologias de reconhecimento facial – TRFs[3], envolvem uma ampla variedade de processos automatizados nos quais são utilizadas representações faciais digitais para tentar identificar ou verificar a identidade de um indivíduo (BUOLAMWINI *et al*, 2020). As TRFs podem ser agrupadas em três categorias mais amplas, a depender da questão que buscam responder: “(a) há um rosto na imagem?; (b) que tipo de rosto há na imagem?; e (c) a quem pertence o rosto na imagem?” (BUOLAMWINI *et al*, 2020. p. 2).

A resposta à pergunta (a) é elementar para a própria detecção de rostos em imagens e não faz nenhuma análise subsequente sobre outros atributos que possam estar associados aos rostos detectados. A resposta a esta pergunta envolve o mapeamento de dados biométricos faciais. As TRFs enfrentam diversos desafios, já que muitos parâmetros influenciam sua performance em ambientes não controlados[4], além dos desafios impostos pelo envelhecimento, expressões faciais, variações de ângulo, escala, oclusão, condições de luminosidade, interferência de fundo da imagem (MOU, 2010; LYNCH, 2018). Já as respostas relativas à (b) buscam avaliar algo sobre o rosto identificado: seu gênero, idade, estado emocional, raça e expressões faciais.

A questão (c), finalmente apresenta a tentativa de estabelecer a identidade de uma pessoa ou se duas imagens representam uma mesma pessoa (BUOLAMWINI *et al*, 2020). Nesta perspectiva, as TRFs de verificação podem tentar determinar se uma imagem mostra uma pessoa em particular, cuja identidade é conhecida, como é o caso dos sistemas de controle de acesso a dispositivos pessoais e serviços; ou se duas imagens mostram a mesma pessoa, caso no qual a identidade delas não é necessariamente conhecida. Ainda no âmbito de (c), há TRFs de identificação, caso no qual o sistema de reconhecimento facial tenta associar um rosto a uma pessoa cujos dados biométricos faciais já constem em um banco de dados/galeria preexistente, podendo gerar uma correspondência ou não.

O processo de reconhecimento facial pode ser dividido em etapas (BUOLAMWINI *et al*, 2020). A captura e detecção relaciona-se com a obtenção da imagem ou fotografia. A circunstância de captura pode ser: para verificação de identidade para acesso a dispositivo ou serviço; em ambientes controlados; de forma voluntária ou não; e ainda a coleta de imagens disponíveis em redes sociais. Já a inscrição, tradução livre de *enrollment*, é o processo de coleta de informação visual de um indivíduo para formação de uma galeria ou banco de dados (BUOLAMWINI *et al*, 2020).

Em seguida, os dados colhidos em etapas anteriores são tratados por algoritmos de reconhecimento facial. Tradicionalmente, algoritmos de reconhecimento podem ser divididos em abordagens geométricas relativas a características fotométricas ou distintivas, permitindo uma classificação entre algoritmos holísticos – aqueles que buscam reconhecer completamente a face – e os métodos *feature-based* – aqueles que analisam características faciais locais (como olhos, nariz e boca) e armazenam parâmetros e métricas como ângulos e distâncias entre os pontos fiduciais no rosto como descritores para comparação futura no processo de reconhecimento facial (GALTERIO *et al*, 2018; JOSHI; GUPTA, 2016; PETRESCU, 2019).

Assim, nesta etapa, as imagens são processadas e transformadas em representações digitais da biometria facial, sendo o objetivo a criação de representações digitais dos rostos presentes nas imagens. Tais representações são chamadas de *faceprints*. Os *faceprints* devem ser desenvolvidos de forma a alcançar a maior acurácia possível para a próxima etapa, que consiste em comparar duas imagens da mesma pessoa (BUOLAMWINI *et al*, 2020). Em um processo de identificação, a etapa de comparação envolve identificar um *faceprint* e compará-lo a outros disponíveis na base de dados/galeria, gerando escores de similaridade, computados para estimar o quão parecidos são dois *faceprints* (BUOLAMWINI *et al*, 2020).

A decisão sobre a correspondência nas TRFs de identificação são as mais relevantes para aplicações em segurança pública, nosso foco no presente artigo. Na obtenção de resultados quanto a correspondência, os processos resultantes de TRFs de identificação indicam vários rostos no banco de dados/galeria que potencialmente correspondem ao rosto submetido (BUOLAMWINI *et al*, 2020). Nos referiremos à lista de resultados como a relação de candidatos à correspondência correta. No Quadro 1 sintetizamos as possíveis respostas à etapa de correspondência.

Quadro 1 – Síntese de possíveis respostas para correspondências

Possíveis Respostas para correspondências
Correspondência correta (*true match*): Como supracitado, processos de identificação envolvem a comparação entre uma amostra e um banco de dados/galeria, processo este que retorna múltiplas correspondências, sendo apenas uma delas verdadeira. Em geral, um operador humano é consultado para comparar resultados e eleger o correto.
Não-Correspondência (*true mismatch*): Indica que o rosto buscado não está presente no banco de dados/galeria, quer dizer, o sistema não possui informação visual daquela pessoa.
Falso-positivo (*false match*): é a associação errônea de amostras de duas pessoas, e ocorre quando os *faceprints* de duas pessoas diferentes são similares. No contexto de identificação por autoridades policiais pode resultar no envolvimento de uma pessoa inocente em uma investigação, por exemplo.
Falso-negativo (*false mismatch*): Ocorre quando se falha em associar a mesma pessoa em duas amostras diferentes. No contexto de identificação por autoridades policiais, um falso negativo pode fazer com que autoridades policiais negligenciem uma pessoa que acreditam ter alguma conexão com um crime.

Fonte: Adaptado de Buolamwini e colaboradores (2020) e de Grother, Ngan e Hanaoka (2019).

A comparação de *faceprints* no processo de identificação resulta no escore, como citado anteriormente. Com base nesse escore, um parâmetro limítrofe pode ser configurado para decidir se dois *faceprints* correspondem ou não entre si. Buolamwini e colaboradores (2020) citam que, se um sistema trabalha com um escore de similaridade de 0 a 100, um parâmetro limítrofe de 80 fará com que apenas *faceprints* aos quais foram atribuídas similaridades iguais ou superiores a 80 sejam considerados como uma correspondência. Isto torna o parâmetro limítrofe um fator crítico para a correção da resposta do sistema. Os autores pontuam que não há configuração de parâmetro limítrofe para a qual as correspondências resultantes sejam isentas de erros (BUOLAMWINI *et al*, 2020). Para processos de identificação, parâmetros limítrofes altos podem aumentar taxas de não-correspondência ou de falsos negativos.

Desta forma, Buolamwini e colaboradores (2020) ponderam que há um *trade-off* associado aos parâmetros limítrofes, tornando pouco significativa a caracterização da precisão de sistemas de identificação facial em um único número. Lynch (2018) aponta que os sistemas de reconhecimento facial operam melhor quando todas as imagens são coletadas com condições de luminosidade similares e de uma perspectiva frontal. Quando as imagens comparadas contêm diferenças significativas de resolução, iluminação, sombra, plano de fundo, poses ou expressões faciais, as taxas de erro se tornam significativas (LYNCH, 2018).

Todas estas particularidades técnicas fazem com que seja difícil criar um índice que possa responder cabalmente sobre a precisão de sistemas de reconhecimento facial, ainda mais considerando que TRFs são um gênero de tecnologias e não uma tecnologia específica, que usam distintos algoritmos de reconhecimento facial e que podem apresentar diferentes tipos de erros, distribuídos iniquamente entre populações demográficas diferentes (GROTHER; NGAN; HANAOKA, 2019). Assim, a avaliação da performance de TFRs envolve diversas variáveis, que podem ser medidas com base em processos estatísticos e concentradas em uma métrica de performance, o que torna o processo complexo. Buolamwini e colaboradores (2020) alegam que a principal armadilha na mensuração da performance das TFRs é supor que as métricas de performance,

construídas com base em bancos de dados/galerias amplas e padronizadas, possam ser representativas da performance do sistema em cenários reais.

Um relatório recente do Laboratório de Tecnologia da Informação da agência de administração de tecnologia dos Estados Unidos, o *National Institute of Standards and Technologys* (NIST), avaliou uma amostra bastante representativa de 189 algoritmos de reconhecimento facial de 99 desenvolvedores, buscando quantificar a precisão de algoritmos de reconhecimento facial por grupos demográficos (definidos pelo sexo, idade, e etnia/país de nascimento). O relatório, de autoria de Grother e colaboradores (2019), foi realizado com intuito de testar os fornecedores de TRFs, pontuou que há uma ampla precisão entre estes, variando conforme o algoritmo principal do sistema, sua aplicabilidade e os dados que o alimentam. Para o Laboratório, os algoritmos mais precisos produzem taxas muito menores de erro (GROTHER; NGAN; HANAOKA, 2019). Um dos destaques do relatório aponta que a maioria dos algoritmos apresenta diferenciais demográficos, ou seja, sua capacidade de associar duas imagens da mesma pessoa varia de um grupo demográfico para outro (GROTHER; NGAN; HANAOKA, 2019), o que pode ser considerado um viés racial e/ou de gênero (BUOLAMWINI, 2017).

Mais especificamente, o relatório mostrou que, no contexto dos diferenciais demográficos, falsos positivos são os erros mais frequentes, chegando a variar de 10 a mais de 100 vezes mais entre grupos demográficos. O relatório enfoca algoritmos individuais, portanto, conclui que diferentes algoritmos funcionam de maneira diferente, obtendo, portanto, resultados diferentes. Entretanto, há uma tendência de que algoritmos de identificação tenham performances pronunciadamente piores para identificar mulheres, sobretudo as de ascendência africana, bem como pessoas asiáticas (GROTHER; NGAN; HANAOKA, 2019).

Esse efeito, é, em geral, amplo entre países, variando ainda conforme o país de desenvolvimento do algoritmo: em algoritmos desenvolvidos na China, o diferencial demográfico favoreceu a precisão entre rostos asiáticos (GROTHER; NGAN; HANAOKA, 2019). Ainda conforme o relatório, outros grupos com altas taxas de falso-positivos foram idosos e crianças. Todos estes complicadores tendem a deixar em aberto a questão de como decidir se uma TRF em especial é apropriada para implantação em uma população-alvo determinada (BUOLAMWINI *et al*, 2020).

RECONHECIMENTO FACIAL NA SEGURANÇA PÚBLICA

As vantagens das TRFs sobre outras modalidades biométricas, a exemplo da invasividade nula, a tornam um alvo em potencial para emprego na vigilância e na segurança pública. Com uma base de dados ampla o suficiente – como tende a ser o caso da Identificação Civil Nacional, criada pela Lei n° 13.444/2017, e em implementação no Brasil –, um sistema de monitoramento seria capaz de identificar, em tempo real, transeuntes anônimos em logradouros públicos através da comparação de pontos faciais registrado no banco de imagens, aplicação esta denominada vigilância facial (tradução livre de *face surveillance*).

Considerando tais aplicações, Petrescu (2019) aponta que sistemas de reconhecimento facial são capazes de prover informação adicional, armazenando parâmetros faciais de cidadãos que posteriormente possam ser confrontados em investigações criminais. Para a autora, tais sistemas “não exigem envolvimento

pessoal prévio para reconhecer um indivíduo, e apenas enxergam dados, e não sexo, idade ou raça", "diminuindo assim a probabilidade de discriminação" (PETRESCU, 2019, p. 243). A autora argumenta que, apesar de a tecnologia não decidir por si própria, seu emprego permitiria promover uma maior transparência no processo de tomada de decisão de autoridades policiais sobre buscas e abordagens (PETRESCU, 2019). Controversamente, Lynch (2018) afirma que, sem treinamento especializado, humanos podem ser piores em identificação facial que um algoritmo de computador, enquanto Garvie e colaboradores (2016) argumentam que a possibilidade de erro humano aumenta à medida que o operador desconheça o sujeito da identificação ou pertença a um grupo étnico diferente daquele.

Como terceira possibilidade de aplicação em segurança pública, há TRFs híbridas, que agregam características de vigilância e identificação. O rastreamento facial (tradução livre de *face tracking*) se caracteriza como o uso policial de imagens de vídeo em tempo real ou gravações para rastrear um suspeito. A principal diferença entre as modalidades é a possibilidade de o rastreamento facial envolver informação de localização sobre determinado suspeito. Para Garvie e colaboradores (2016) o reconhecimento facial em tempo real tem o potencial nocivo de redefinir a natureza de espaços públicos.

Apesar de apresentar taxas cada vez menores de erro em testes controlados, como o do NIST (2019), as TRFs ainda apresentam os supracitados diferenciais demográficos, variando conforme desenvolvedor e algoritmo principal, não atingindo precisão total. Os vieses, representados pelos diferenciais demográficos se dão, também em função da composição do banco de dados/galeria de base para o algoritmo de identificação. Buolamwini e Gebru (2018) reforçaram a existência de diferença na exatidão do reconhecimento facial em relação ao gênero e raça.

A controvérsia aumenta ainda mais quando se discute taxas de acerto em situações reais, como é o caso da aplicação da tecnologia no ramo da segurança pública. Se testes controlados analisam o desempenho de algoritmos atuando sobre bases de dados/galerias em condições ideais (amostras de igual luminosidade, pose, resolução etc.) as taxas de acerto podem variar amplamente considerando aplicações em situações reais. É o que relatórios recentes da organização britânica *Big Brother Watch*¸ apontam: uma maioria das correspondências obtidas utilizando dados de reconhecimento facial automatizado foram incorretas (BIG BROTHER WATCH, 2018). Em média 93% das correspondências obtidas pelo sistema de vigilância em tempo real da Polícia Metropolitana de Londres foram imprecisas (BIG BROTHER WATCH, 2020).

Além disso os percentuais de erro variam largamente em função da TRF em questão. Rastreamento facial, por exemplo, envolve taxas de erro mais altas, por representar desafios técnicos ainda maiores devido à coleta de dados em ambientes não controlados. Para Lynch (2018), questões técnicas endêmicas a todas TRFs indicam que os erros continuarão a ser um problema comum no futuro próximo. A questão é que, "virtualmente, há um conjunto ilimitado de condições sob as quais TRFs podem ser usadas", enquanto seus índices de avaliação de desempenho operam e modelam com base em um número restrito de aplicações (LEARNED-MILLER *et al*, 2020).

Neste sentido, tais índices de avaliação de desempenho das TRFs avaliam apenas como elas irão operar em condições que refletem o banco de dados

utilizado (LEARNED-MILLER *et al*, 2020). O desempenho da TRF vai depender da proporção em que o banco de dados reflita a diversidade da população alvo do emprego da tecnologia, uma vez que é mais difícil distinguir dentro de um grupo populacional mais homogêneo (LEARNED-MILLER *et al*, 2020).

Enquanto tais questões permanecem em aberto, é suposto que dentre os propalados benefícios do uso de TRFs na segurança pública, sobretudo em contextos de vigilância, estaria a possibilidade de localizar criminosos, extremistas e crianças desaparecidas (GALTERIO *et al*, 2018). Nos Estados Unidos, a ONG *Thorn* já ajudou a identificar, com emprego de reconhecimento facial, mais de 10 mil vítimas de tráfico sexual de crianças, as resgatando e protegendo da divulgação de pornografia infantil[5]. Por outro lado, 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, ocorridos ao 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.

Liberdades civis também foram ameaçadas nos Estados Unidos, onde TRFs foram empregadas para coletar dados e rastrear ativistas em protestos recentes do movimento *Black Lives Matters* (SELINGER; CAHN, 2020; VINCENT, 2020), demonstrando que o emprego de reconhecimento facial para fins de vigilância e controle não é prerrogativa exclusiva de Estados com características ditatoriais como a China – da qual Hong Kong é uma região administrativa especial –, mas é vastamente empregado também em Estados democráticos de direito, como é o caso dos Estados Unidos.

As controvérsias técnicas e patentes abusos envolvendo emprego de tecnologias de reconhecimento facial na segurança pública apontam para a necessidade de regulação desta tecnologia. Somente a regulamentação de seu emprego pode fornecer orientações para uma implementação que respeite diferentes setores, com regras apropriadas que considerem riscos e benefícios. Neste sentido, autores do campo jurídico indicam a necessidade de interação da regulamentação com a autorregulação ou corregulação das empresas do ramo (FRAZÃO, 2019b).

RECONHECIMENTO FACIAL NO CONTEXTO BRASILEIRO

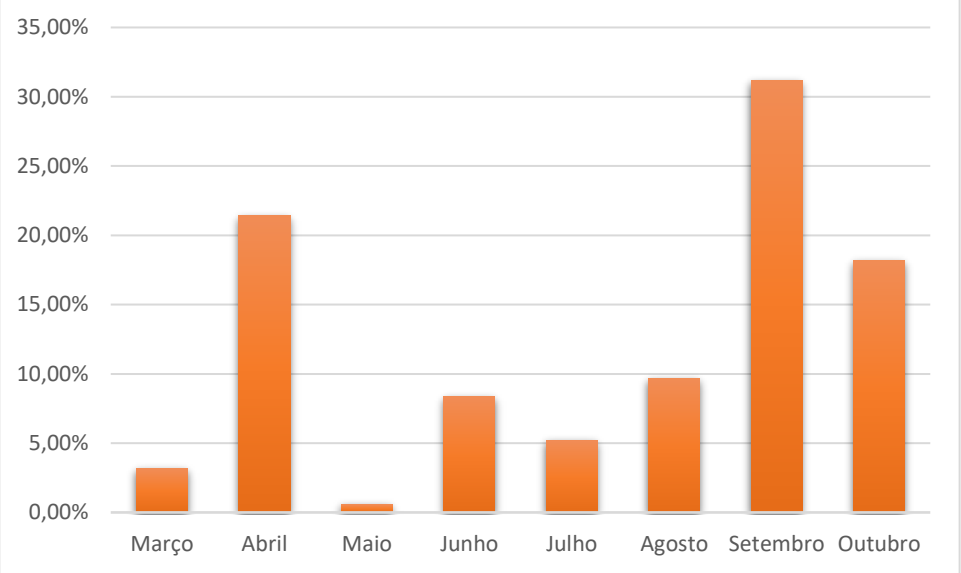
A compreensão, mesmo que superficial, dos meandros técnicos envolvidos nas TRFs é importante sobretudo para perceber adequadamente sua ambivalência. Debates éticos, jurídicos e sociais já presentes em países do norte global se intensificam no cenário nacional, a partir da adoção de sistemas de monitoramento 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 do ano de 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[6].

O cruzamento destes dados com imagens captadas em locais de crime e fragmentos de impressões digitais são enviadas para uma equipe especializada, que submete o material à análise com emprego da nova tecnologia, supostamente diminuindo as margens de erro para identificação de suspeitos. A tecnologia 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, demonstrada na Figura 1, requer um debate qualificado, considerando não apenas os benefícios, mas também os riscos envolvidos (NUNES, 2019).

Figura 1 - Prisões efetuadas com o uso de RF na Bahia, Rio de Janeiro, Santa Catarina e Paraíba (março a outubro de 2019).



Fonte: Adaptado da Nunes (2019).

Considerando os vieses que as TRFs podem incorporar, há uma notória preocupação entre cientistas sociais e juristas de que o emprego de reconhecimento facial possa reforçar a seletividade do sistema penal brasileiro (SILVA; SILVA, 2019). Algoritmos, neste sentido, a menos que usados de modo muito cuidadoso, podem perpetuar e reforçar preconceitos (KELLEHER; TIERNEY, 2018).

Turow (2013) já descrevia processos através dos quais a ciência de dados categorizava pessoas para fins de marketing, resultando em tratamento preferencial para alguns e marginalização para outros. Eubanks (2017) também se dedicou a explicar como algoritmos ajudam a automatizar a desigualdade, uma vez que o escrutínio digital pelo qual passamos não é individual, senão coletivo no sentido de que os indivíduos são analisados enquanto membros de grupos sociais.

Minorias oprimidas e exploradas “carregam um fardo um fardo muito maior de monitoramento e rastreamento do que grupos favorecidos” (EUBANKS, 2017, p. 11). Grupos marginalizados são submetidos a uma maior coleta de dados em situações cotidianas, dados estes que reforçam a marginalização de seus titulares

quando usados para os tornar suspeitos e sujeitos a um escrutínio maior, configurando um círculo vicioso (EUBANKS, 2017), retroalimentando a injustiça social vigente.

Neste sentido, deve-se contestar a suposta objetividade da ciência de dados, que, por ser baseada em números seria incapaz de codificar preconceitos ou incorporá-los. Conforme pontuam Kelleher e Tierney (2018), algoritmos são frutos de abstrações, sendo, portanto, incapazes de corresponder a descrições objetivas do mundo, incorporando parcialidade e vieses.

Assim, algoritmos funcionam de modo amoral, e não-objetivo: a ciência de dados extrai padrões de dados, entretanto, se tais dados codificarem relações de preconceito na sociedade, então o algoritmo provavelmente irá identificar tal padrão, passando a basear nele seus resultados, ou seja, os refletindo. Para os autores, quanto mais consistente um preconceito na sociedade, mais acentuado será sua influência nos dados sobre aquela sociedade, tornando mais provável que um algoritmo científico o extraia e replique (KELLEHER; TIERNEY, 2018). Este fato torna-se ainda mais problemático no caso do uso de algoritmos para policiamento e segurança pública.

Enfocando a realidade sócio-histórica brasileira segundo a parcialidade dos algoritmos, destaca-se, em seus mais de 300 anos de escravidão, o racismo estrutural da sociedade brasileira, que se projeta nos resultados obtidos com o emprego do reconhecimento facial. Nunes (2019) destaca, por exemplo, que durante o carnaval de Feira de Santana, na Bahia, o sistema de videomonitoramento capturou os rostos de mais de 1,3 milhões de foliões, gerando 903 alertas que resultaram na prisão de 15 pessoas, gerando uma imprecisão de 96%dos alertas. Essa e outras pesquisas mostram que homens brancos são reconhecidos com mais assertividade pela tecnologia do que mulheres negras (TAUTE, 2020). Silva e 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.

Conforme Pinheiro (2020), a informação é um dos ativos mais valiosos de que dispomos, e a proteção de dados, prioridade absoluta. No campo ético, sublinhamos que a biometria facial é a mais vulnerável em termos de coleta sem autorização prévia, sendo capaz de oferecer uma enorme quantidade de dados e informações pessoais que podem ser utilizados para fins obscuros. Neste campo, percebe-se que a amplitude de possibilidades de uso das TRFs cria nichos de mercado novos, altamente rentáveis, como é o caso da segurança pública, sem, contudo, ser acompanhado por garantias quanto ao emprego ético e responsável, tanto por parte de governos quanto por parte de empresas.

A falta de normatização e regulação adequada pode favorecer o uso ilegal de dados pessoais, donde a necessidade de mecanismos de controle, amplamente debatidos, com participação da sociedade civil organizada, que garantam à sociedade participação no processo de conformação de parâmetros éticos e sua observação (OLIVEIRA, 2020).

REGULAÇÃO E MECANISMOS DE CONTROLE: A LGPD E O USO DE DADOS BIOMÉTRICOS PARA FINS PENAIS

As práticas de vigilância trazem à baila a necessidade de avanço dos dispositivos jurídicos e legais de modo a formar um arcabouço consistente para "lidar com a aceleração do desenvolvimento tecnológico, buscando estabilidade e segurança" (LOUREIRO; CARNEIRO, 2020, p. 221). Entretanto, os desafios para regular o setor são enormes: a contraposição entre o princípio jurídico da territorialidade e o fluxo globalizado de dados (WEBER, 2012); a rápida obsolescência à que estão sujeitas matérias de alto teor técnico ou especializado e o risco de que normas demasiado abstratas impeçam a efetivação de direitos a elas relacionados. (LOUREIRO; CARNEIRO, 2020).

No que tange especificamente a questão dos dados pessoais, é importante lembrar que estes não constituem bens de cunho exclusivamente patrimonial. Daí a "insuficiência das soluções de mercado para qualquer disposição a respeito deles" (FRAZÃO, 2019, p. 103)[7]. A proteção de dados, incluindo os biométricos, compõe um direito fundamental autônomo calcado no princípio da liberdade e da dignidade humana, o que torna inaceitável tratar indivíduos como objeto de constante vigilância (FRAZÃO, 2019b).

Neste sentido, a criação de um marco legal para proteção de dados pessoais no Brasil está em debate pelo menos desde meados de 2010 tendo resultado, oito anos mais tarde, em 2018, na sanção da principal referência nacional sobre o tema, a Lei Geral de Proteção de Dados LGPD – Lei Nº 13.709, de 14 de agosto de 2018. A entrada em vigor seguiu prazos diversos a depender do artigo em questão, sendo que os prazos de vigência geral foram protelados diversas vezes por leis posteriores.

Assim, a LGPD é o principal, senão o único, mecanismo de controle jurídico plenamente dedicado à proteção de dados pessoais de que o país dispõe. 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 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 Lei Geral de Proteção de Dados brasileira (PINHEIRO, 2020).

A coleta e utilização de dados biométricos para identificação, por exemplo, através da instalação de sistemas de reconhecimento facial em locais públicos, acarreta riscos específicos para os direitos fundamentais que podem variar consideravelmente em função do objetivo, contexto e âmbito desta utilização. Neste sentido, os regulamentos de proteção de dados da União Europeia já proíbem o tratamento de dados biométricos com o objetivo de identificar uma pessoa de forma individual, exceto em condições específicas (COMISSÃO EUROPEIA, 2020).

A LGPD dispõe sobre o tratamento de dados pessoais da pessoa natural e busca "reforçar a autonomia informativa e a dignidade dos titulares dos dados, bem como a própria democracia" (FRAZÃO, 2019a). Conceituando juridicamente os dados pessoais como sendo quaisquer informações relacionadas a pessoa natural identificada ou identificável (art. 5º, I), públicos ou tornados públicos pelos seus titulares, a LGPD 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).

Seu objetivo, portanto, é o de proteger amplamente o cidadão quanto às situações relevantes que porventura sejam afetadas pelo tratamento de dados, (art. 5º, X), inclusive nos meios digitais, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (FRAZÃO, 2019b). Portanto, a LGPD atua como um "freio e um agente transformador das técnicas atualmente utilizadas pelo capitalismo de vigilância, a fim de conter a maciça extração de dados e as diversas aplicações e utilizações que a eles podem ser dadas sem a ciência ou o consentimento informado dos usuários" (FRAZÃO, 2019b, p. 103).

Consoante o art. 4º, inciso III, alíneas "a" e "d", a LGPD não é aplicável ao tratamento de dados com fins exclusivos de segurança pública ou de atividades de investigação e repressão de infrações penais. A informalmente chamada "LGPD-Penal" [8], visa disciplinar o tratamento de dados pessoais no âmbito da segurança pública, investigações penais e repressão de infrações penais e já possui anteprojeto de lei, fruto do trabalho de uma comissão de juristas instituída pela Câmara do Deputados em novembro de 2019[9]. Tal legislação deverá, observando o devido processo legal e princípios gerais de proteção e os direitos do titular previstos na LGPD, prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público (TEFFÉ; FERNANDES, 2020).

A necessidade de regulação desta atividade se baseia sobretudo na atividade prática de órgãos responsáveis por atividades de segurança pública e de investigação/repressão criminais, que atualmente não detêm segurança jurídica para utilizar TRFs, de modo a respeitar garantias processuais e os direitos fundamentais dos titulares dos dados envolvidos. A falta de parâmetros claros e transparentes acaba por reforçar disparidades e assimetrias de poder entre o cidadão e o Estado em questões de persecução criminal, visto que o crescimento acentuado das novas técnicas de vigilância e investigação viabilizam o estabelecimento de um altíssimo grau de monitoramento e vigilância.

Na ausência da votação e vigência da "LGPD-Penal", a LGPD permanece sendo a única referência em âmbito nacional para a questão. Tendo em vista a importância de conteúdos guardados em determinadas informações e a potencialidade de seu uso servir para fins discriminatórios contra o indivíduo (TEFFÉ; FERNANDES, 2020), a LGPD trata dados biométricos como sendo dado pessoal sensível, quando vinculado a uma pessoa natural (art. 5º, II). A este tipo de dado é dispensada uma proteção específica mais rígida, em um rol próprio de bases legais (art. 11). Outro ganho importante da LGPD para o uso de dados biométricos, é servir de referência para gerar uma maior coordenação entre os entes federados que até então regulam somente sistemas já em operação.

Quanto aos fundamentos e princípios orientadores da LGPD, constantes nos artigos 2º e 6º, as previsões da LGPD compartilham princípios constitucionais e direitos fundamentais, em interlocução com o Código Civil e com o Código de Defesa do Consumidor (FRAZÃO, 2019b). Um de seus eixos valorativo é a noção de privacidade[10] que surge em conexão com as noções de igualdade e não-discriminação, em consideração aos reconhecidos efeitos discriminatórios das decisões algorítmicas (O'NEIL, 2016; EUBANKS, 2017; AGRAWAL; GANS; GOLDFARB, 2018; KELLEHER; TIERNEY, 2018), especialmente quando tais decisões ocorrem integralmente de forma automatizadas, sem garantia de intervenção humana.

Neste quesito, algumas nuanças da entrada em vigor da LGPD ocultou um flagrante retrocesso na proteção de direitos individuais: no âmbito das decisões totalmente automatizadas. A LGPD, em sua redação original previa, segundo o art. 20 que o titular dos dados teria a revisão por pessoa natural de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses. A Medida Provisória 869/2018 foi responsável por suprimir a referência à pessoa natural, permitindo que a "insurgência do titular de dados seja também decidida por uma máquina, sujeitando-o novamente a processos decisórios totalmente automatizados, ainda que em diferentes esferas" (FRAZÃO, 2019c).

Se a LGPD foi um marco, suas contribuições não são suficientes para responder aos desafios impostos pelo uso de TRFs na segurança pública em particular. É necessário instrumentalizar os princípios apontados pela LGPD. A ausência de uma regulação ou orientação de alcance geral, somada ao fato de que bases de dados públicas e privadas – algumas contendo informações detalhadas sobre as vidas civil e penal das pessoas – já coletavam registros biométricos faciais mesmo antes do país aprovar a sua lei de proteção de dados pessoais (INSTITUTO IGARAPÉ, 2019), o que confirma a preocupação sobre o caráter ético do emprego desta tecnologia. Seu uso, atualmente apoiado em uma autorização tácita e regulamentada por estado, carece de uma autoridade central de modo a oferecer maior garantia quanto a coibição de riscos potenciais (FRANCISCO; HIUREL; RIELLI, 2020).

Assim como qualquer outra tecnologia emergente (ROTOLO; HICKS; MARTIN, 2015), o reconhecimento facial representa uma novidade radical com crescimento relativamente rápido, capaz de causar impactos proeminentes de forma incerta e ambígua. Regular o uso de uma tecnologia emergente é complexo e deve preservar direitos civis sem privar a sociedade de eventuais benefícios da inovação, sem que se tenha exata clareza dos possíveis impactos daquela tecnologia (FRANCISCO, HUREL, RIELLI, 2020). Um agravante importante é o fato de que a avaliação de tecnologias muitas vezes só é viável *a posteriori*. No caso do emprego de TRFs à segurança pública, outro agravante é o fato de que envolve instituições públicas, que são diretamente responsáveis pela preservação do interesse da sociedade (FRANCISCO; HIUREL; RIELLI, 2020).

CONSIDERAÇÕES FINAIS

A vigilância constante à qual estamos submetidos é um fato. A banalização do uso do reconhecimento facial é capaz de afetar severamente direitos e garantias fundamentais (TEFFÉ; FERNANDES, 2020). A LGPD, "assim como qualquer outra lei geral de tratamento de dados, obviamente endereça apenas o núcleo central do problema, sem prejuízo de que outras áreas ou leis" (FRAZÃO, 2019b). A despeito da ampla utilização do reconhecimento facial no país, já tendo chegado a 20 estados[11], a legislação da qual dispomos atualmente não sana uma série de dúvidas quanto ao uso dos dados biométricos, sobretudo para fins de segurança pública e investigação/repressão criminais, criando um vácuo normativo o que dificulta ainda mais o debate sobre os limites do emprego de dados sensíveis nesta seara.

Reino Unido, Estados Unidos e França constituem referências para a proteção de dados pessoais e regulação de tecnologias de processamento de dados

biométricos. Suas regulações serviram de referência para a LGPD, e continuam orientando, por exemplo, nossa contraparte brasileira, a incipiente “LGPD-Penal”. O que podemos aprender com o panorama internacional quanto às tendências de regulação dos sistemas de reconhecimento facial é que, mesmo países com uma “longa história de utilização de tecnologias de videomonitoramento, os esforços de regulação ainda estão no começo” (FRANCISCO; HIUREL; RIELLI, 2020, p. 18). Eles nos ensinam o exercício da cautela, ao reconhecer os perigos desta tecnologia, não devendo sua capacidade “se sobrepor aos riscos já identificados” (FRANCISCO; HIUREL; RIELLI, 2020, p. 18), ainda mais considerando o estado da técnica em que se encontra. Neste sentido, um apontamento importante é o desenvolvimento tecnológico autóctone, adequado à cultura do país, que poderia mitigar falhas oriundas de diferenciais demográficos geradores de vieses nos algoritmos empregados.

Além das polêmicas que cercam o emprego do reconhecimento facial, aqui introdutória e brevemente apresentadas, seu uso deve ser antecedido de debate amplo e público, multissetorial, respaldado por valores constitucionais e éticos, no que a LGPD também oferece princípios não suficiente, mas úteis e que devem ser observados. Tal debate é a única garantia de que os instrumentos regulatórios possam contemplar a “perspectiva de especialistas e de todos os grupos potencialmente afetados pelo emprego da tecnologia, garantindo assim a proteção de dados e a elaboração de estratégias para mensurar impactos” (FRANCISCO; HIUREL; RIELLI, 2020, p. 17).

Concluímos apontando que, ao instituir a Autoridade Nacional de Proteção de Dados, a LGPD deixou um indicativo de qual ente pode conduzir tais debates e fomentar a discussão sobre tais temas. Embora saibamos que infraestruturas regulatórias para tecnologias complexas sejam de difícil construção, é premente que a atuação da Autoridade Nacional de Proteção de Dados trate das especificidades das TRFs, considerando riscos e benefícios e coordene as abordagens de regulação desta tecnologia, sobretudo em aplicações de alto risco, como é o caso da segurança pública.

Law enforcement use of face recognition technology in Brazil: ethical, legal and technical aspects

ABSTRACT

Facial recognition is a daily used skill in our lives. Since 1960, when research began, until today, at an increasingly accelerated pace, there is interest in enabling the automated processing of digital images for facial recognition, which can be used in a wide range of applications, including surveillance and public safety. This bibliographical-documentary research seeks to analyze the impacts of the use of facial recognition in public security in Brazil – considering its ethical, legal, technical and social aspects, in order to discuss mechanisms of legal, ethical and social control. The conclusion indicates the need for broader debates, in which, in addition to the technical aspects, other aspects can be considered to achieve a more qualified discussion of the use of technology, especially regarding the current expansion of its use by public authorities throughout the country.

KEYWORDS: Public Security in Brazil. Facial recognition. Surveillance. Artificial Intelligence.

NOTAS

[1] O campo de estudos Ciência, Tecnologia e Sociedade (CTS) estuda, ao menos desde a década de 1960, as relações entre a tecnologia e a sociedade, entregando análises complexas sobre a não-neutralidade da tecnologia ante o processo social (FEENBERG, 1991), investigando o conteúdo político de artefatos técnicos (WINNER, 1980; 1993; BIJKER; PINCH, 1989) e as controvérsias decorrentes de seu emprego. Derivados do objeto específico da tecnologia para vigilância e suas relações com liberdade e controle, surgem os Estudos de Vigilância, "campo de investigação específico para a compreensão dos problemas relativos às tecnologias de vigilância e suas dinâmicas estruturantes na sociedade contemporânea" (PERON; ALVARÉZ; CAMPELLO, 2018, p. 14)

[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 palmares (JAIN; FLYNN; ROSS, 2008).

[3] Do ponto de vista técnico, podemos afirmar que sistemas de reconhecimento facial operam em dois estágios básicos: (a) extração e seleção de características; e (b) classificação de objetos (PETRESCU, 2019). Desenvolvimentos posteriores introduziram outras tecnologias aos procedimentos, que hoje podem, além dos métodos tradicionais, incluir: TRFs tridimensionais, câmaras termais, análise da textura da pele e a combinação destes métodos para o reconhecimento físico (GALTERIO et al, 2018; PETRESCU, 2019).

[4] "Ambiente não controlado" é a tradução livre de *unconstrained enviroments*, e significa a captura de imagens em ambientes em que a imagem do sujeito é capturada em um contexto espontâneo — na rua, no transporte público, entre outras.

[5]. Dados fornecidos pelo relatório de 2018 no site da ONG Thorn: <https://www.thorn.org/impact-report-2018/>. Acesso em 17/05/2020.

[6] Fonte: <https://www.saopaulo.sp.gov.br/spnoticias/governo-inaugura-laboratorio-de-reconhecimento-facial-e-digital-da-policia-civil/> Acesso em 21/07/2021.

[7] "[...] o mercado de dados em geral cresce a partir da difusão de visões como a de que o modelo de negócios é justo, já que os usuários receberiam contrapartidas adequadas pelos seus dados, ou mesmo necessário, dado que haveria um verdadeiro trade off entre inovação e privacidade, de maneira que a violação desta última seria o preço a pagar ou o mal necessário para o progresso tecnológico e os novos serviços que daí decorrem. Até a forma como a questão é apresentada já reflete a perspectiva utilitarista que permeia a análise, pois se parte da premissa de que, em nome da inovação, é justificável o sacrifício de direitos fundamentais elementares papel de reforçar a autonomia informativa dos titulares dos dados e o necessário e devido controle que estes precisam exercer sobre os seus dados, a fim de se colocar um freio nas vicissitudes que possibilitaram a consolidação do estágio atual da economia movida a dados" (FRAZÃO, 2019a, p. 31).

[8] A legislação pretende complementar o microssistema legislativo de tratamento de dados para fins de segurança pública e de investigação criminal, atualmente

presente em leis esparsas, voltadas sobretudo à regulamentação de quebras de sigilo no contexto processual penal.

[9] Fonte: <https://static.poder360.com.br/2020/11/DADOS-Anteprojeto-comissao-protecao-dados-seguranca-persecucao-FINAL.pdf> Aceso em 21/07/2021.

[10] Tradicionalmente restrita à intimidade e ao direito de ser deixado só, a noção de privacidade corrente precisa ser atualizada para se encontrar "compatível com a complexidade dos desafios inerentes à economia movida a dados e à vigilância" (FRAZÃO, 2019b, p. 105). Discussões atuais sobre o tema consideram a compreensão da privacidade em conexão com outros direitos ou garantias fundamentais, abarcando "o controle sobre as informações que digam respeito ao sujeito, a autodeterminação informativa, o direito à não discriminação, a liberdade, a igualdade, o direito ao acesso e acompanhamento dos dados pessoais quando se tornam objeto de disponibilidade de outros, dentre outros" (FRAZÃO, 2019b, p. 107), voltando-se para as noções de cidadania e dignidade.

[11] Fonte: <https://www1.folha.uol.com.br/cotidiano/2021/07/sob-criticas-por-vies-racial-reconhecimento-facial-chega-a-20-estados.shtml>. Acesso em 21/07/2021.

AGRADECIMENTOS

Agradecemos aos editores da Revista Tecnologia e Sociedade e aos avaliadores anônimos por seus comentários em versões anteriores deste artigo.

REFERÊNCIAS

AGRAWAL, A.; GANS, J.; GOLDFARB, A. **Prediction machines**. The simple economics of artificial intelligence. Boston: Harvard Business Review Press, 2018.

BIG BROTHER WATCH. **Big Brother Watch Briefing on facial recognition surveillance**. Big Brother Watch, 2020. Disponível em <https://bigbrotherwatch.org.uk/wp-content/uploads/2020/06/Big-Brother-Watch-briefing-on-Facial-recognition-surveillance-June-2020.pdf> Acesso em 17 out. 2021.

BIG BROTHER WATCH. **Face Off**: The lawless growth of facial recognition in UK policing. Big Brother Watch, 2018. Disponível em <https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf > Acesso em 17 out. 2021.

BIJKER, W. E.; PINCH, T. F. The Social Construction of Facts and Artifacts: Or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other. In: BIJKER, W. E.; HUGHES, T. P.; PINCH, T. F. **The Social Construction of Technoiogical Systems** - New Directions in the Sociology and History of Technology, Massachusetts: MIT Press, p. 17-50, 1989.

BUOLAMWINI, J. **Gender shades**: intersectional phenotypic and demographic evaluation of face datasets and gender classifiers. 2017. Tese de Doutorado. Massachusetts Institute of Technology.

BUOLAMWINI, J.; GEBRU, T. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. **Proceedings of Machine Learning Research**, [s. l.], v. 81, p. 15, 2018.

BUOLAMWINI, J.; ORDÓÑEZ, V.; MORGENSTERN, J; LEARNED-MILLER, E. L. **Facial Recognition Technologies**: A Primer. Algorithmic Justice League, 2020. Disponível em < https://www.ajl.org/federal-office-call > Acesso em 17 out. 2021.

COMISSÃO EUROPEIA. LIBRO BLANCO. **Sobre la inteligencia artificial** - un enfoque europeo orientado a la excelencia y la confianza. Bruselas: [s. n.], 2020.

EUBANKS, V. **Automating inequality**. How high-tech tools profile, police, and punish the poor. New York: St. Martin's Press, 2017

FARIA, I. C. G. Segurança pública brasileira: responsáveis, números e desafios. **Politize**. Publicado em 13 de junho de 2018. Última atualização em 10 de abril de 2019. Disponível em: <https://www.politize.com.br/seguranca-publica-brasileira-entenda/> Acesso em 20/07/2020.

FEENBERG, A. **Critical theory of technology**. New York: Oxford University Press, 1991.

FONTES, E. O que você precisa saber sobre a Lei Geral de Proteção de Dados Pessoais. **Revista Segurança Eletrônica**, v. 4, n. 40, Maio de 2020. Disponível em <https://issuu.com/revistasegurancaeletronica/docs/revista_se_ed40_completa> Acesso em 01/06/2020.

FOUCAULT, M. **Microfísica do Poder**. São Paulo: Paz e Terra, 2014.

FOUCAULT. M**. Vigiar e punir**: nascimento da prisão. Petrópolis: Vozes, 2011.

FRANCISCO, P. A. P.; HUREL, L. M.; RIELLI, M. M. **Regulação do reconhecimento facial no setor público: avaliação de experiências internacionais**. [s.l.]: Instituto Igarapé + Data Privacy Brasil Research, 2020. Disponível em: https://igarape.org.br/wp-content/uploads/2020/06/2020-06-09-Regulação-do-reconhecimento-facial-no-setor-público.pdf. Acesso em: 17/07/2021.

FRAZÃO, A. Fundamentos da proteção dos dados pessoais - Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de dados. In: G. Tepedino, A. Frazão, M. D. Oliva. (Org.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. 1ed.São Paulo: Thomson Reuters - Revista dos Tribunais, 2019a.

FRAZÃO, A. Nova LGPD. Balanço preliminar da MP 869/2018. **Jota**. 2019c. Disponível em: [www.jota.info/paywall?redirect_to=//www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-balanco-preliminar-da-mp-869-2018-06022019]. Acesso em: 20.07.2021.

FRAZÃO, A. Objetivos e alcance da Lei Geral de Proteção de Dados. In: Gustavo Tepedino, Ana Frazão, Milena Donato Oliva. (Org.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. 1ed.São Paulo: Thomson Reuters - Revista dos Tribunais, 2019b.

GALTERIO, M.; SHAVIT, S.; HAYAJNEH, T. A Review of Facial Biometrics Security for Smart Devices. **Computers**, v. 7, n. 3, 2018.

GARVIE, C; BEDOYA, A.; FRANKLE, J. **The perpetual line-up**: unregulated police face recognition in America. New Jersey: Center on Privacy & Technology at Georgetown Law, 2016. Disponível em: <https://www.perpetuallineup.org/>, Acesso em: 17/05/2020.

GROTHER, P.; NGAN, M.; HANAOKA, K. **Face Recognition Vendor Test (FRVT) Part 3**: Demographic Effects. National Institute of Standards and Technology, 2019. doi.org/10.6028/NIST.IR.8280

INSTITUTO IGARAPÉ. **Infográfico de reconhecimento facial no Brasil**, 2019. Disponível em: <https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/>, Acesso em: 17 maio de 2020.

JAIN, A. K.; ROSS, A. Introduction to Biometrics. In: Jain, AK; Flynn, P; Ross, A (org.). **Handbook of Biometrics**. New York: Springer, 2008.

JOSHI, J. C.; GUPTA, K. K. Face Recognition Technology: A Review. **The IUP Journal of Telecommunications**, v. 8, n. 1, 2016, pp. 53-63.

KELLEHER, J. D.; TIERNEY, B. **Data Science**. Cambridge: The MIT Press, 2018.

LEARNED-MILLER, E.; ORDÓÑEZ, V.; MORGENSTERN, J; BUOLAMWINI, J. **Facial Recognition Technologies in the Wild**: A Call for a Federal Office. Algorithmic

Justice League, 2020. Disponível em <https://www.ajl.org/federal-office-call> Acesso em 18 out. 2021.

LOUREIRO, M. F. B.; CARNEIRO, J. V. V. Problematizando o direito à privacidade e à proteção de dados pessoais em face da vigilância biométrica. **Teknokultura**, v. 17, n. 2, p. 205-213, 2020.

LYNCH, J. **Face Off**: Law Enforcement Use of Face Recognition Technology. Electronic Frontier Foundation, 2018. Disponível em <https://www.eff.org/files/2018/02/15/face-off-report-1b.pdf > Acesso em 17 out. 2021.

MOU, D. **Machine-based Intelligent Face Recognition**. Beijing: Higher Education Press, 2010.

NUNES, P. Novas ferramentas, velhas práticas: reconhecimento facial e policiamento no Brasil. In: Rede De Observatórios da Segurança. **Retratos da violência cinco meses de monitoramento, análises e descobertas**, pp. 67–71, 2019. Disponível em: <http://observatorioseguranca.com.br/wordpress/wp-content/uploads/2019/11/1relatoriorede.pdf> Acesso em 18 nov. 2021.

O'NEIL, Cathy. **Weapons of math destruction**: how big data increases inequality and threatens democracy (edição eletrônica). New York: Crown, 2016.

OLIVEIRA, G. P. S. Sigilo de dados no brasil: da previsão constitucional à nova lei geral de proteção de dados pessoais. **Revista Âmbito Jurídico**, n 193 – Ano XXII – Fevereiro/2020.

PASQUALE, F. **The black box society**: the secret algorithms that control money and information. Massachusetts: Harvard University Press, 2015.

PERON, A. E. R.; ALVAREZ, M. C.; CAMPELLO, R. U. Apresentação do Dossiê: Vigilância, Controle e Novas tecnologias. **Mediações**, Londrina, v. 23 n. 1, p. 11-31, 2018.

PETRESCU, R. V.R. Face Recognition as a Biometric Application. **Journal of Mechatronics and Robotics**, v.3, s.n., 2019.

PINHEIRO, P.P. Qual o impacto da LGPD em instituições de ensino e pesquisa? **Rede Nacional de Pesquisa e Ensino** (RNP). Publicado em maio/2020. Disponível em <https://www.rnp.br/noticias/qual-o-impacto-da-lgpd-em-instituicoes-de-ensino-e-pesquisa>. Acesso em 06/06/2020.

ROTOLO, D.; HICKS, D.; MARTIN, B. R. What is an emerging technology?. **Research Policy**, v. 44, n. 10, 2015.

SELINGER, E.; CAHN, A. F. Did you protest recently? Your face might be in a database. **The Guardian**. 17 jun. 2020. Disponível em: < https://www.theguardian.com/commentisfree/2020/jul/17/protest-black-lives-matter-database> Acesso em 16 out. 2021.

SILVA, R. L.; SILVA, F. S. R. Reconhecimento Facial e segurança pública: os perigos do uso da tecnologia no sistema penal seletivo brasileiro. **Anais do 5 Congresso Internacional de Direito e Contemporaneidade**: mídias e direitos da sociedade em rede. UFSM - Universidade Federal de Santa Maria. 2019.

SRNICEK, N. **Platform capitalism**. Cambridge: Polity Press, 2018.

TAUTE, F. Reconhecimento facial e suas controvérsias. **Heinrich Boll Stiftung**. Rio de Janeiro, 2020.

TEFFÉ, C. S.; FERNANDES, E; R. Reconhecimento Facial: laissez-faire, regular ou banir? **Migalhas**, 16 de jul. de 2020. Disponível em < https://www.migalhas.com.br/coluna/migalhas-de-vulnerabilidade/330766/reconhecimento-facial--laissez-faire--regular-ou-banir> Acesso em 17/07/2021.

TUROW, J. **The Daily You**: How the New Advertising Industry Is Defining Your Identity and Your Worth. New Haven, CT: Yale University Press, 2013.

VINCENT, J. NYPD used facial recognition to track down Black Lives Matter activist. **The Verge**. 18 ago. 2020. Disponível em: <https://www.theverge.com/2020/8/18/21373316/nypd-facial-recognition-black-lives-matter-activist-derrick-ingram> Acesso em 16 out. 2021.

WEBER, R. H. How Does Privacy Change in the Age of the Internet?. In: A. Albrechtslund; K. Boersma; C. Fuchs **Internet and Surveillance**: The Challenges of Web 2.0 and Social Media (, pp. 273-295). New York: Routledge, 2012.

WINNER, L. Upon Opening the Black Box and Finding It Empty: Social Constructivism and the Philosophy of Technology. **Science, Technology, & Human Values**, v. 18, n. 3, p. 362-378, 1993.

Recebido: 07/08/2020
Aprovado: 23/11/2021
DOI: 10.3895/rts.v18n50.12968

Como citar: OLIVEIRA, L.V. et al. Aspectos ético-jurídicos e tecnológicos do emprego de reconhecimento facial na segurança pública no Brasil**. Rev. Tecnol. Soc**., Curitiba, v. 18, n. 50, p.114-135, jan./mar., 2022. Disponível em: https://periodicos.utfpr.edu.br/rts/article/view/12968. Acesso em: XXX.

Correspondência: