BREVES CONSIDERAÇÕES ACERCA DA UTILIZAÇÃO DO RECONHECIMENTO FACIAL COMO INSTRUMENTO DE SEGURANÇA PÚBLICA E PERSECUÇÃO

BRIEF CONSIDERATIONS ABOUT THE USE OF FACIAL RECOGNITION AS AN INSTRUMENT OF PUBLIC SAFETY AND PROSECUTION

Renan Barboza de Faria
Doutorando e Mestre em Direito Processual Penal pela USP. Bacharel em Direito pela FMU. Assistente Jurídico do TJ-SP. Membro do IBCCRIM.
Link Lattes: http://lattes.cnpq.br/9222185855891560
ORCID: https://orcid.org/0000-0002-8496-3570
renanbarboza@hotmail.com

Renatha Gonçalves da Mota e Silva
Graduanda em Direito pela UNINASSAU
Link Lattes: http://lattes.cnpq.br/3337710589339737
ORCID: https://orcid.org/0000-0002-7299-1662
renathamotta_@hotmail.com

Resumo: O artigo realiza breve análise da adoção do reconhecimento facial como reação à sofisticação da criminalidade. Objetiva-se traçar o panorama da utilização dessa tecnologia no Brasil e suas principais dificuldades, sobretudo considerando a desproporcional ingerência em direitos fundamentais.

Palavras-chave: Segurança pública; Tecnologia; Reconhecimento facial; Imprecisão; Racismo.

Abstract: The article does a brief analysis of the adoption of facial recognition as a reaction to crime sofistication. The objective is to outline the outlook of this technology usage in Brazil and its main difficulties, especially considering the disproportionate interference with fundamental rights.

Keywords: Public safety; Technology; Facial recognition; Imprecision; Racism.

1. O desenvolvimento tecnológico e a adequação dos mecanismos de prevenção e repressão

As transformações do mundo contemporâneo foram construídas mediante a incidência da modernização tecnológica, que buscava produzir velocidade nos processos e na comunicação. Nesse sentido, as práticas ilícitas também foram favorecidas, aprimorando as condutas já existentes e incidindo no surgimento de novas, em que a sensação de liberdade e impunidade proporcionada pela criação do ambiente virtual impactou o crescimento e propagação de ações e discursos de ódio, compra e venda de ilícitos, além da quebra de privacidade, que se tornou cada vez mais comum, com a invasão, sequestro e divulgação de dados, que buscam a exposição pública ou favorecimento de outros crimes.

À vista disto, destaca-se como a modernização tecnológica, trazendo à tona um modelo de comunicação muito mais acessível, permitiu a facilitação na organização de ações criminosas, bem como na manipulação de informações, principalmente no âmbito virtual. Nota-se também que, além da sofisticação tecnológica, a criminalidade também se utiliza das fragilidades sociais para prática de infrações.

Tal cenário permite notar também a paulatina substituição da criminalidade clássica, caracterizada pela limitação a ambientes físicos, pela criminalidade praticada no ciberespaço ou com a utilização de métodos atualizados e que dificultam sua apuração, tratando-se, assim, de verdadeiro fenômeno de busca por espaços de oportunidade criminosa (MIRÓ-LLINARES; MONEVA, 2019, p. 3).

Este fenômeno ao mesmo tempo estabeleceu forçadamente aos Estados a necessidade de adequação dos métodos de busca e produção de provas aos avanços da tecnologia da informação e comunicação, exigindo novas perspectivas na forma e regulamentação dos procedimentos de apuração e prevenção de delitos, trazendo à tona, inclusive, uma postura reativa, buscando a incorporação de novos mecanismos e técnicas de investigação e controle, bem como atualização daquelas já existentes, sobretudo com a introdução da inteligência artificial, sob o pretexto da obtenção e análise eficiente de dados. Um dos usos da inteligência artificial para fins de prevenção e repressão de delitos se verifica no reconhecimento facial.

2. Apontamentos acerca do sistema de reconhecimento facial e sua implementação no Brasil

Conforme indicado, o veloz desenvolvimento tecnológico, sobretudo nas áreas da comunicação e vigilância, levou à busca incessante da sociedade por segurança, permitindo a incorporação de sistemas de reconhecimento facial às câmeras de monitoramento utilizadas tanto em locais públicos como privados. Diante do crescimento na utilização dessa tecnologia, o debate acerca de sua incorporação em larga escala têm assumido relevância.

Normalmente apontado como exemplo de mecanismo eficiente de gestão de risco e apuração de delitos, sua implementação é defendida sob a justificativa da segurança pública, sem que sejam indicados maiores esclarecimentos acerca das precauções de sua utilização, certamente redutora de direitos fundamentais. Esse tipo de tecnologia tem como grande ponto negativo a opacidade, ou seja, a dificuldade (e até impossibilidade) de verificação e reprodução do *iter* de funcionamento de sistemas que utilizam técnicas de *machine learning* (MIRÓ-LLINARES, 2018, p. 113).

Importante destacar que esse mecanismo é uma forma de identificação biométrica, um processo que possibilita a identificação ou verificação da identidade a partir de características físicas ou comportamentais inerentes a uma pessoa. Entretanto, a captura de dados parte de inúmeras fontes (câmeras de vigilância, celulares, etc.), que operam de forma incessante e, principalmente, sem que o titular do dado perceba. Essas características são fundamentais para possibilitar o rastreamento secreto e massificado por reconhecimento facial.

O procedimento de reconhecimento facial para identificação e localização estrutura-se em quatro fases: inicia-se com a utilização de um algoritmo que permite a localização do rosto da pessoa na imagem (detecção); em seguida, há o dimensionamento e alinhamento da face para comparação com as demais processadas pelo algoritmo (preparação); posteriormente, o algoritmo extrai as características da face que podem ser quantificadas de forma numérica, como a distância entre os olhos, nariz e boca ou a textura da pele (extração de características); na fase final de identificação, o algoritmo examina grupos de imagens de rostos e emite uma pontuação que reflete o grau de identificação entre as faces cadastradas no sistema e aquela submetida à identificação (GARVIE; BEDOYA; FRANKLE, 2016, p. 9).

Destaca-se que essa análise é possível apenas porque o sistema passou por procedimento de *machine learning* supervisionado. Tal aprendizado, com a utilização de dados testes, embora traga ganhos significativos na velocidade de obtenção de resultados de identificação, o faz sacrificando valores como transparência e explicabilidade, além de outros princípios que deveriam nortear a aplicação de sistemas de reconhecimento facial.

"[...] A CAPTURA DE DADOS PARTE DE INÚMERAS FONTES (CÂMERAS DE VIGILÂNCIA, CELULARES, ETC.), QUE OPERAM DE FORMA INCESSANTE E, PRINCIPALMENTE, SEM QUE O TITULAR DO DADO PERCEBA."

Considerando a realidade brasileira, segundo relatório do Instituto Igarapé, a utilização de sistemas de reconhecimento facial no Brasil em diferentes áreas é reportada pelo menos desde 2011 (INSTITUTO IGARAPÉ, 2019). Na cidade de São Paulo, por exemplo, constata-se o uso de câmeras de reconhecimento facial no sistema de transporte público desde 2017 (GARAY, 2019, p. 7).

Entretanto, nota-se grande dificuldade no acesso às informações sobre os impactos da implementação dessa tecnologia, cuja regulamentação caminha a passos lentos e na contramão de outros países, que inicialmente procuraram estabelecer premissas básicas para sua utilização (NUNES, 2019, p. 70).

Diante dessa situação, a utilização do reconhecimento facial tem como garantias mínimas em nosso país aquelas previstas na Lei Geral de Proteção de Dados (Lei 13.709/2018 - LGPD), uma vez que o dado biométrico é expressamente reconhecido como dado pessoal e de natureza sensível. Contudo, apesar dos princípios gerais de proteção e direitos do titular previstos pela LGPD serem plenamente aplicáveis ao uso de reconhecimento facial, a referida lei excepciona sua incidência no tratamento de dados para manutenção de segurança pública e persecução/apuração de delitos.

Em 2019, dois decretos presidenciais (Decreto 10.046/2019 e Decreto 10.047/2019) possibilitaram a criação de uma grande base unificada e compartilhada de dados pessoais dos cidadãos. Os decretos ilustram os atuais riscos de implementação e normalização de sistemas de vigilância em massa, uma vez que permitem o armazenamento de dados biométricos faciais, associados a diversos outros dados biográficos.

Esse cenário, acrescido da implementação do reconhecimento facial, apresenta sérios riscos a direitos fundamentais, tais como: precisão na identificação; impactos desproporcionais na identificação de pessoas; impacto em liberdades públicas; e descontrole na retenção e utilização de dados pessoais.

3. Riscos apresentados pelo uso do reconhecimento facial

3.1 Precisão na identificação e descontrole na utilização de dados pessoais

Sistemas de reconhecimento facial normalmente podem desempenhar três tipos de funções. O sistema pode ser concebido para identificar uma pessoa desconhecida; para verificação de identidade (sistemas de liberação de acesso); e para localização de múltiplas faces previamente identificadas (LYNCH, 2020, p. 5).

Importante ressaltar que, em vez de identificar positivamente uma pessoa desconhecida com um único resultado, muitos sistemas de reconhecimento facial são desenvolvidos para calcular a probabilidade de identificação entre a pessoa desconhecida e as inúmeras fotos armazenadas em uma base de dados, dando como resultado múltiplos potenciais correspondentes, ranqueados de acordo com o grau de probabilidade da identificação correta (LYNCH, 2020, p. 6).

Isso pressupõe que todo sistema de reconhecimento facial deveria comunicar sua taxa de erros, incluindo o número de falsos positivos e falsos negativos. O falso positivo ocorre em situações nas quais o sistema acusa a correspondência da face de uma pessoa com uma das imagens armazenadas em uma base de dados, porém tal correspondência não é verdadeira. O falso negativo, por outro lado, verifica-se na hipótese de falha do sistema em encontrar uma imagem correspondente à face submetida à comparação, porém há, de fato, uma imagem correspondente armazenada na base de dados.

O sistema de reconhecimento facial, portanto, deve ser desenvolvido para operar almejando o menor grau possível de falsos positivos, uma vez que a ocorrência do falso negativo é menos danosa à sociedade.

Considerando ainda a utilização em massa do reconhecimento facial, a coleta e armazenamento de grande quantidade de dados pessoais pode incrementar riscos à segurança dessas informações, ainda que retidos em bases de dados governamentais.

Embora recente, é notável o crescimento na utilização de sistemas de reconhecimento facial e seu emprego em diversos ramos da segurança pública e também na administração geral do estado para identificação de pessoas e prestação dos mais diversos serviços (como banco de dados utilizados para controle de habilitações para condução de veículos). Dessa forma, a utilização de sistemas integrados, embora eficiente para a prestação dos serviços, pode acarretar brechas externas e internas de segurança e causar a exposição ou alteração de dados pessoais, de sorte que é necessária maior transparência do Estado acerca da implementação, utilização e aproveitamento dos resultados.

"[...] MUITOS SISTEMAS DE RECONHECIMENTO FACIAL SÃO DESENVOLVIDOS PARA CALCULAR A PROBABILIDADE DE IDENTIFICAÇÃO ENTRE A PESSOA DESCONHECIDA E AS INÚMERAS FOTOS ARMAZENADAS EM UMA BASE DE DADOS [...]"

3.2 Impacto em liberdades públicas

Eventuais violações aos direitos fundamentais em razão de decisões discriminatórias que venham a ser tomadas pelo sistema, carecem de meios inteligíveis de justificação e verificação. Tal situação, especialmente em relação à preservação da segurança pública, pode atingir severamente a liberdade dos indivíduos.

A privacidade é uma das faces da liberdade mais atingidas pela utilização do reconhecimento facial. Considerando-a como a capacidade de controle do indivíduo sobre seus dados pessoais sem, contudo, esquecer a necessidade de relacionamento com terceiros (LEONARDI, 2012, p. 88), a mera possibilidade de registro em qualquer lugar e de submissão à verificação por sistema de reconhecimento facial, sujeitando-se, portanto, aos problemas apontados nos tópicos anteriores, representa, por si só, desmesurada violação, caracterizando indevida vigilância e podendo resultar na afetação de outras formas de liberdade diante de detenções e acusações injustificadas.

É comum o raciocínio de que a utilização de câmeras em locais públicos não feriria o direito à privacidade, uma vez que os indivíduos nesses espaços não teriam expectativa a esse direito, pois optaram por publicamente expor seus rostos. O equívoco nesse pensamento é considerar que a informação sensível em jogo é apenas a face dos indivíduos, ou seja, não se considera para qual finalidade é empregada a tecnologia, uma vez que a face é meramente o objeto de análise para a extração de diversas outras informações, em relação às quais não houve a intenção do indivíduo de apresentar publicamente e em relação às quais certamente há expectativa de privacidade (HIROSE, 2017, p. 1604), carcaterizando verdadeira obtenção sub-reptícia de dados sensíveis sem prévia autorização judicial.

3.3 Impactos desproporcionais na identificação de pessoas negras

Considerado uma extensão dos problemas de precisão, uma vez que sua gênese está na obtenção de falsos positivos, faz-se necessário analisar o impacto social da utilização do reconhecimento facial, ponderando o viés racial enraizado em nossa política penal. Visto que a sociedade brasileira experimenta, na ótica de **Sueli Carneiro** (2005, p. 43), o dispositivo racialidade, que descreve bem a disparidade de tratamento policial e jurídico para pessoas negras. Assim, elenca-se o questionamento se a referida tecnologia ajudaria a reduzir o racismo estrutural.

Pesquisas mostram que o reconhecimento de pessoas negras tendem a apresentar falsos positivos no comparativo de imagens (KLARE *et al.*, 2012, p. 1799; WHITTAKER, 2018, p. 16). Como exemplo, temos a tecnologia utilizada pelo Google, que reconheceu como

pessoas negras imagens de gorilas e objetos. Logo, a utilização do reconhecimento facial como instrumento probatório e de segurança certamente contribuiria no crescimento de prisões arbitrárias, além de facilitar as violências comuns em abordagens policiais, perpetuando a coação social (SILVA; SILVA, 2019).

Nesse sentido, as falhas destacadas acima reforçam o tratamento preconceituoso a pessoas negras, que têm o tom de sua pele correlacionado à criminalidade, de forma que o incentivo à utilização da tecnologia pelo Estado, desconsiderando sua imprecisão, além de naturalizar desigualdades sociais, enfatizaria sua responsabilidade pela distinção racial de tratamento, transmitindo à sociedade a aceitabilidade dessas violências.

Ainda, a utilização e divulgação do reconhecimento facial antes do reconhecimento pessoal na fase investigativa influenciaria diretamente na produção de falsas memórias, aumentando os riscos de criminalização indevida, principalmente em relação à população negra.

O maior número de imagens de pessoas negras em bases de dados utilizadas para comparação também acarreta desproporcional desvantagem na utilização do reconhecimento facial para checagem de antecedentes em outras searas (como o mercado de trabalho), sobretudo diante da desatualização de dados provenientes de sistemas de Persecução Penal (LYNCH, 2020, p. 10).

Em pesquisa realizada pelo *National Institute of Standards and Technology*, na qual foram avaliados 189 algoritmos de 99 desenvolvedores de reconhecimento facial para medir as ocorrências de falsos positivos e falsos negativos, foi verificada maior taxa de falsos positivos para rostos asiáticos, negros e indígenas quando comparado a pessoas brancas. Ainda segundo esse estudo, mulheres negras representam o grupo mais atingido (GROTHER; NGAN; HANAOKA, 2019).

Segundo apontado anteriormente, o reconhecimento facial depende do treinamento de inteligência artificial, de sorte que esse sistema sempre estará sujeito à dificuldade de verificação do caminho utilizado pela máquina para tomada de decisão na comparação de imagens e apresentação de resultados.

Assim, a análise e controle da utilização do sistema se revela muito dificultosa, pricipalmente a tarefa de despi-la de viéses preconceituosos, ainda que não tenham pautado a criação do sistema.

4. Conclusão

Embora pouco retratada em nosso ordenamento jurídico, a tecnologia do reconhecimento facial já é utilizada no Brasil desde 2017, contudo, com pouca ou nenhuma informação acerca de sua implementação, funcionamento e limites que deveriam pautar sua utilização.

Embora apresentada como sinônimo de eficiência na segurança pública, de todos os sistemas biométricos, esse é o que tem as mais altas taxas de falsos positivos e falsos negativos, o que acaba comprometendo demasiadamente sua eficácia e afetando diretamente direitos fundamentais, como o direito à privacidade, o tratamento de dados sensíveis, além de liberdades públicas em geral diante de identificações equivocadas.

Considerando, ainda, que as taxas elevadas de falsos positivos afetam, sobretudo, grupos já marginalizados socialmente, como pessoas negras e mulheres, comprometendo não só medidas de segurança pública e repressão de crimes, como também a eventual persecução, o uso de tecnologias de reconhecimento facial revela-se especialmente arriscado em contextos nos quais determinados grupos já são historicamente objeto de tratamento discriminatório, funcionando mais como instrumento de perpetuação do racismo do que de segurança pública.

Referências

ABBAS DA SILVA, Lorena.; FRANQUEIRA, Bruna Diniz; HARTMANN, Ivar A. O que os olhos não veem, as câmeras monitoram: reconhecimento facial para segurança pública e regulação na América Latina. *Revista Digital de Direito Administrativo*, v. 8, n. 1, p. 171-204, 2021. DOI: 10.11606/issn.2319-0558.v8i1p171-204. Disponível em: https://www.revistas.usp.br/rdda/article/view/173903. Acesso em: 16 nov. 2022.

ALMEIDA, Silvio. *Racismo estrutural*. São Paulo: Sueli Carneiro; Pólen, 2019.

ARAÚJO, Rômulo de Aguiar; CARDOSO, Naiara Deperon; PAULA, Amanda Marcélia de. Regulação e uso do reconhecimento facial na segurança pública do Brasil. *Revista de Doutrina Jurídica*, v. 112, p. e021009, 2021. DOI: 10.22477/rdj.v112i00.734. Disponível em: https://revistajuridica.tjdft.jus.br/index.php/rdj/article/view/734. Acesso em: 16 nov. 2022.

BOTELLO, Nelson Arteaga. Regulación de la videovigilancia en Mexico. Gestión de la ciudadanía y acceso a la ciudad. *Espiral* (Guadalajara), v. 23, n. 66, may./ago. 2016. Disponível em: https://bit.ly/2SxQBkJ. Acesso em: 20 jan. 2022.

CARNEIRO, Sueli. *A construção do outro como não-ser como fundamento do ser*. 2005, 339 p. Tese (Doutorado em Educação) – Universidade de São Paulo, São Paulo, 2005.

FERREIRA, Lucia Maria Teixeira. *Parecer sobre a legalidade dos Decretos nº 10.046/2019 e 10.047/2019*. Rio de Janeiro, 17 jan. 2020. Disponível em: https://bit.ly/3fNDiH7. Acesso em: 16 nov. 2022.

GARAY, Vladimir. Mal de ojo: reconocimiento facial en América Latina. *In:* DERECHOS DIGITALES. *Latin America in a Glimpse*, p. 1-9, nov. 2019. Disponível em: https://www.derechosdigitales.org/wp-content/uploads/glimpse-cap-rec-facial.pdf. Acesso em: 20 jan. 2022.

GARVIE, Clare; BEDOYA, Alvaro; FRANKLE, Jonathan. The perpetual line-up: unregulated police face recognition in America. *Georgetown Law Center on Privacy & Technology*, out. 2016. Disponível em: https://www.perpetuallineup.org. Acesso em: 20 nov. 2021.

GROTHER, Patrick; NGAN, Mei; HANAOKA, Kayee. *NIST Interagency/Internal Report (NISTIR) 8280 - Face recognition vendor test (FRVT)*. Part 3: Demographic Effects. NIST, Dez. 19, 2019.

HIROSE, Mariko. Privacy in public spaces: the reasonable expectation of privacy against the dragnet use of facial recognition technology. *Connecticut Law Review*, v. 49, n. 5, sep. 2017.

INSTITUTO IGARAPÉ. *Reconhecimento facial no Brasil*. Desde 2011 vem sendo utilizado o reconhecimento facial no Brasil. 2019. Disponível em: https://bit.ly/2L89rvh. Acesso em: 20 jan. 2022.

KLARE, Brendan F.; BURGE, Mark J.; KLONTZ, Joshua C.; BRUEGGE, Richard W. Vorder ; JAIN, Anil K. Face recognition performance: role of demographic information. *IEEE Transactions on Information Forensics and Security*, v. 7, n. 6, p. 1789-1801, Dec. 2012. Disponível em: http://openbiometrics.org/publications/klare2012demographics.pdf. Acesso em: 20 nov. 2021.

LEONARDI, Marcel. *Tutela e privacidade na internet*. São Paulo: Saraiva, 2012.

LYNCH, Jennifer. Face off: law enforcement use of face recognition technology. *Electronic Frontier Foundation*, Apr. 20, 2020. Disponível em: https://www.eff.org/pt-br/wp/law-enforcement-use-face-recognition. Acesso em: 16 nov. 2022.

MIRÓ-LLINARES, Fernando. Inteligencia artificial y justicia penal: más allá de los resultados lesivos causados por robots. *Revista de Derecho Penal y Criminología*, UNED, 3ª época, v. 20, p. 87-130, 2018. DOI: https://doi.org/10.5944/rdpc.20.2018.26446

MIRÓ-LLINARES, Fernando; MONEVA, Asier. What about cyberspace (and cybercrime alongside it)? A reply to Farrell and Birks "Did cybercrime cause the crime drop?" *Crime Science*, v. 8, n. 12, 2019. Disponível em: https://crimesciencejournal.biomedcentral.com/articles/10.1186/s40163-019-0107-y. Acesso em: 21 nov. 2022.

NUNES, Pablo. 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. CESeC, jun./out. 2019, p. 67-70. Disponível em: http://observatorioseguranca.com.br/wordpress/wp-content/uploads/2019/11/1relatoriorede.pdf. Acesso em: 16 nov. 2022.

SILVA, Rosane Leal da; SILVA, Fernanda dos Santos Rodrigues da. Reconhecimento facial e segurança pública: os perigos do uso da tecnologia no sistema penal seletivo brasileiro. *In*: CONGRESSO INTERNACIONAL DE DIREITO E CONTEMPORANEIDADE, 5., 2019, Santa Maria. *Anais* [...]. Santa Maria, RS: UFSM, 2019. Disponível em: https://www.ufsm.br/app/uploads/sites/563/2019/09/5.23.pdf. Acesso em: 16 nov. 2022.

WHITTAKER, Meredith *et al. AI Now Report 2018*. Dec. 2018. Disponível em: https://ainowinstitute.org/AI_Now_2018_Report.pdf. Acesso em: 16 nov. 2022.

Recebido em: 15.08.2022 - Aprovado em: 20.10.2022 - Versão final: 29.11.2022