

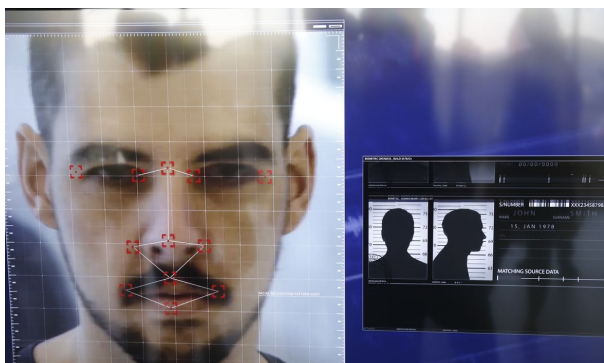
Gabrielle Cenci: Reconhecimento facial pela IA no CPP brasileiro

20/06/2023

O verbo "reconhecer" remonta suas raízes etimológicas ao latim *recognoscere*: conhecer novamente, retomar o significado, trazer mais uma vez à mente. Não por outro motivo, o reconhecimento — seja de coisas ou de pessoas — adota uma posição central em um processo penal compreendido justamente como um ato (*re*)*cognitivo*, ou seja, de "*reconstrução aproximativa de um determinado fato histórico*" [1].

E, sob esta perspectiva, deve ser tratado com cautela, sob pena de macular a formação de convencimento do julgador na atividade de conhecer (novamente) do fato apurado. Assim, torna-se pleonasma afirmar que se faz necessário regulamentar estritamente o procedimento de reconhecimento no bojo da persecução penal, na mesma esteira do que vem entendendo o Superior Tribunal de Justiça desde a mudança de paradigma firmada no Habeas Corpus nº 598.886/SC.

Fernando Frazão/Agência Brasil



Fernando Frazão/Agência Brasil

Entretanto, a despeito do novo entendimento da obrigatoriedade de observância das disposições do artigo 226 do Código de Processo Penal na produção probatória, é certo que a legislação processual penal não se estende para abranger um problema trazido pelo panorama da quarta revolução industrial: o impacto da inteligência artificial no procedimento de reconhecimento de pessoas. E isto não é surpreendente — afinal, o Código de Processo Penal data de 1941 e, apesar das inúmeras reformas parciais às quais esteve sujeito nestas décadas (e que mantiveram o espírito inquisitorial do processo penal brasileiro, não compatível com a Constituição de 1988 [2]), ainda peca em trazer qualquer disposição sobre a prova digital.

Neste ponto, especificamente, são inúmeras as discussões sobre o cabimento e os riscos sociais das tecnologias de *digital surveillance*, das quais estas breves considerações irão se eximir. Sem embargo, basta compreender que o clássico modelo do panóptico — uma prisão circular com celas escuras e uma torre de vigia no centro [3], para gerar um senso de autovigilância e

controle comportamental [4] — foi meramente mais um dos processos automatizados no século 21, gerando o panóptico digital [5].

Hoje, já não se pode mais precisar o alcance das tecnologias (e de como estas são utilizadas para angariar informações para fins de *surveillance*) no cotidiano. Desde o reconhecimento facial para desbloquear a tela do *smartphone* até o uso de biometria em terminais de autoatendimento bancários: tudo compõe um grupo massivo de informações interligadas conhecido como *Big Data*, que irá alimentar os algoritmos de inteligência artificial para os mais diversos objetivos — inclusive o de docilizar o comportamento social e proporcionar a vigilância e a punição dos transgressores.

A empresa Surfshark, que atua no setor de segurança cibernética, realizou um levantamento que aponta que 109 países empregam ou aprovaram o emprego a ser implementado de alguma forma de tecnologia de reconhecimento facial para fins de segurança, do total de 194 países mapeados [6].

Nas festividades de Carnaval da Bahia, em 2023, quase 80 foragidos foram presos com o auxílio de câmeras de reconhecimento facial [7]. Embora estes casos digam respeito à mera localização de pessoas contra as quais haja mandado de prisão ativo e, a partir da semelhança, notifique a polícia, não parece distante cogitar que estas mesmas câmeras possam identificar um indivíduo em flagrante delito — e, justamente por isso, tornarem-se meio de prova no processo penal.

Em cotejo com o artigo 226 do Código de Processo Penal e com o Habeas Corpus nº 598.886/SC, ainda, é possível afirmar que, hoje, um reconhecimento pessoal realizado por uma inteligência artificial *tecnicamente* poderia ser admitido como prova. Não seria difícil pedir ao algoritmo que descrevesse a pessoa a ser reconhecida, a partir de um comando básico de transposição da imagem em texto (inciso I). No mesmo sentido, o posicionamento do sujeito ao lado de outras pessoas com quem possua semelhança para que seja efetuado o reconhecimento também parte do funcionamento básico da máquina: a comparação de informações (inciso II). E, em se tratando de uma inteligência artificial, ao menos em tese, não haveria o risco de intimidação ou influência (inciso III).

Todavia, ser *tecnicamente* possível observar as determinações do artigo 226 do CPP não significa dizer que a prova deva ser, de fato, admitida ao processo penal. Não se desconhece que as análises produzidas por algoritmos são tidas como objetivas e, portanto, imunes a qualquer questionamento, até mesmo porque a maior parte da população não tem o conhecimento matemático para impugná-las [8]. Este é o efeito *black box* dos algoritmos — pela complexidade inerente a este tipo de tecnologia, não há transparência em seu funcionamento, que atua de maneira opaca, tal qual a caixa-preta de um avião [9]. E não é só: para além da falta de opacidade nas inteligências artificiais, o eventual uso do reconhecimento facial algorítmico como prova no processo penal ainda esbarra em, pelo menos, dois outros questionamentos: a proteção dos dados utilizados para o processo de aprendizado de máquina e a existência comprovada de vieses raciais que prejudicam seu funcionamento.

O reconhecimento facial digital funciona a partir do mapeamento de pontos do rosto do indivíduo cuja imagem é capturada e da comparação destes dados biométricos com informações

preexistentes em um banco de dados [10] — que, no caso do uso desta tecnologia pelos órgãos de segurança pública, pode ser composto pelas fotografias dos documentos de identidade (RG) ou da Carteira Nacional de Habilitação (CNH). É evidente que isto gera um gravoso problema justamente quanto à esfera pessoal dos titulares destes dados; afinal, a Lei Geral de Proteção de Dados (Lei nº 13.709/18) especificamente exclui de sua proteção o tratamento de dados pessoais para fins de segurança pública, defesa nacional, segurança do Estado, e de investigação e repressão de infrações penais (artigo 4º, III). E mais: seria possível garantir a cadeia de custódia de uma prova produzida com base nestes dados? Afinal, qual sua fiabilidade, quando inúmeros são de falsidades ideológicas que levam à geração de documentos falsos?

Em outro giro, ainda, o reconhecimento pessoa pela inteligência artificial também padece de outro conhecido vício. Em 2019, um estudo tecido pelo *National Institute of Standards and Technology*, parte integrante do *U.S. Department of Commerce*, demonstrou que algoritmos de identificação facial são mais propensos a resultar em falsos positivos quando o alvo compõe algum grupo racializado, especialmente negros e asiáticos, e também quando se trata de mulheres, crianças ou idosos [11]. Noutras palavras: o reconhecimento facial é confiável, mas apenas para o homem branco adulto. É de se recordar que, em 2021, menos da metade da população brasileira (43%) se declarou branca [12]. Assim, mais uma vez, questiona-se: é possível conferir valor probatório efetivo a uma prova produzida com base em um banco de dados que não corresponde com a realidade?

Em apertada síntese, o que se observa é que, embora o Código de Processo Penal seja defasado em relação às novas metodologias de investigação digital, o reconhecimento facial algorítmico não violaria frontalmente o artigo 226 em uma primeira leitura. Entretanto, as peculiaridades do funcionamento deste tipo de modelo matemático computacional exigem que, ao menos, sejam sopesadas as delicadas questões que surgem, sob pena de deixar-se de observar direitos processuais mínimos que devem ser assegurados ao indivíduo – seja em tempos de processo penal digital ou analógico.

Independentemente da (in)admissibilidade do reconhecimento pessoal produzido por uma inteligência artificial, parece que a mera existência de tecnologias de controle tão precisas e tão presentes no cotidiano resguarda uma assustadora semelhança com a distopia *orwelliana* descrita na obra 1984: um *big brother* apto a assistir, onipresente e onisciente, a todos os movimentos da sociedade.

[1] LOPES JR., Aury. *Direito Processual Penal*. 17ª ed. São Paulo: Saraiva, 2020. p. 556.

[2] GIACOMOLLI, Nereu José. Algumas marcas inquisitoriais do Código de Processo Penal brasileiro e a resistência às reformas. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, vol. 1, nº 1, p. 143-165, 2015. p. 144.

[3] BENTHAM, Jeremy. *O Panóptico*. 2ª ed. Belo Horizonte: Autêntica, 2000. p. 20.

[4] FOUCAULT, Michel. *Vigiar e Punir: nascimento da prisão*. 2ª ed. Petrópolis: Vozes, 1983. p. 177.

[5] HAN, Byung Chul. *No Enxame: perspectivas do digital*. Edição Digital. Petrópolis: Vozes, 2018. p. 66.

[6] Disponível em: <<https://surfshark.com/facial-recognition-map>>. Acesso em: 09 jun. 2020.

[7] Disponível em: <<https://g1.globo.com/fantastico/noticia/2023/02/26/com-ajuda-de-cameras-de-reconhecimento-facial-77-foragidos-da-policia-sao-presos-no-carnaval-da-bahia.ghtml>>. Acesso em: 09 jun. 2023.

[8] O'NEIL, Cathy. *Algoritmos de Destruição em Massa: como o Big Data aumenta a desigualdade e ameaça a democracia*. Tradução de Rafael Abraham. Santo André, SP: Editora Rua do Sabão, 2020. p. 07/08.

[9] "In computing, a 'black box' is a system for which we know the inputs and outputs but can't see the process by which it turns the former into the latter. Somewhat confusingly, airplane flight recorders are also referred to as black boxes; when an artificially intelligent system is indecipherable, it is like an airplane black box for which we have no key" (MICHEL, Arthur Holland. *The Black Box, Unlocked: predictability and understandability in military AI*. Genebra: United Nations Institute for Disarmament Research (UNIDIR), 2020. p. 03).

[10] NEGRI, Sergio Marcos Carvalho de Ávila; OLIVEIRA, Samuel Rodrigues de; COSTA, Ramon Silva. O Uso de Tecnologias de Reconhecimento Facial Baseadas em Inteligência Artificial e o Direito à Proteção de Dados. *RDP*, Brasília, Volume 17, n. 93, 82-103, maio/jun. 2020. p. 86.

[11] GROTH, Patrick. NGAN, Mei; HANAOKA, Kayee. *Face Recognition Vendor Test (FRVT). Part 3: Demographic Effects*. NISTIR 8280. [S.l.]: U.S. Department of Commerce, National Institute of Standards and Technology, 2019. Disponível em: <<https://doi.org/10.6028/NIST.IR.8280>>. Acesso em: 09 jun. 2023.

[12] INSTITUTO Brasileiro de Geografia e Estatística (IBGE). *Pesquisa Nacional por Amostra de Domicílios Contínua 2012/2021*. Disponível em: <https://educa.ibge.gov.br/images/educa/jovens/populacao/22_pnadAtualizacao_jovens_003_corERaca.j>. Acesso em: 09 jun. 2023.

Fonte: <https://conjur.jumps.com.br/2023-jun-20/gabrielle-cenci-reconhecimento-facial-ia-cpp-brasileiro/>