II CONGRESSO INTERNACIONAL DE DIREITO E INTELIGÊNCIA ARTIFICIAL

DIREITO PENAL E CIBERCRIMES

D597
Direito Penal e Cibercrimes [Recurso eletrônico on-line] organização Congresso Internacional de Direito e Inteligência Artificial: Skema Business School – Belo Horizonte;

Coordenadores: Fernando Henrique da Silva Horita; Fausto Santos de Morais; Camila Martins de Oliveira. – Belo Horizonte:Skema Business School, 2021.

Inclui bibliografia
ISBN: 978-65-5648-263-7
Modo de acesso: www.conpedi.org.br
Tema: Um olhar do Direito sobre a Tecnologia

1. Direito. 2. Inteligência Artificial. 3. Tecnologia. II. Congresso Internacional de Direito e Inteligência Artificial (1:2021 : Belo Horizonte, MG).

CDU: 34

II CONGRESSO INTERNACIONAL DE DIREITO E INTELIGÊNCIA ARTIFICIAL

DIREITO PENAL E CIBERCRIMES

Apresentação

Renovando o compromisso assumido com os pesquisadores de Direito e tecnologia do Brasil, é com grande satisfação que a SKEMA Business School e o CONPEDI – Conselho Nacional de Pesquisa e Pós-graduação em Direito apresentam à comunidade científica os 12 livros produzidos a partir dos Grupos de Trabalho do II Congresso Internacional de Direito e Inteligência Artificial (II CIDIA). As discussões ocorreram em ambiente virtual ao longo dos dias 27 e 28 de maio de 2021, dentro da programação que contou com grandes nomes nacionais e internacionais da área em cinco painéis temáticos e o SKEMA Dialogue, além de 354 inscritos no total. Continuamos a promover aquele que é, pelo segundo ano, o maior evento científico de Direito e Tecnologia do Brasil.

Trata-se de coletânea composta pelos 255 trabalhos aprovados e que atingiram nota mínima de aprovação, sendo que também foram submetidos ao processo denominado double blind peer review (dupla avaliação cega por pares) dentro da plataforma PublicaDireito, que é mantida pelo CONPEDI. Os oito Grupos de Trabalho originais, diante da grande demanda, se transformaram em doze e contaram com a participação de pesquisadores de vinte e um Estados da federação brasileira e do Distrito Federal. São cerca de 1.700 páginas de produção científica relacionadas ao que há de mais novo e relevante em termos de discussão acadêmica sobre a relação da inteligência artificial e da tecnologia com os temas acesso à justiça, Direitos Humanos, proteção de dados, relações de trabalho, Administração Pública, meio ambiente, formas de solução de conflitos, Direito Penal e responsabilidade civil.

Os referidos Grupos de Trabalho contaram, ainda, com a contribuição de 36 proeminentes professoras e professores ligados a renomadas instituições de ensino superior do país, os quais indicaram os caminhos para o aperfeiçoamento dos trabalhos dos autores. Cada livro desta coletânea foi organizado, preparado e assinado pelos professores que coordenaram cada grupo. Sem dúvida, houve uma troca intensa de saberes e a produção de conhecimento de alto nível foi, mais uma vez, o grande legado do evento.

Neste norte, a coletânea que ora torna-se pública é de inegável valor científico. Pretende-se, com esta publicação, contribuir com a ciência jurídica e fomentar o aprofundamento da relação entre a graduação e a pós-graduação, seguindo as diretrizes oficiais. Fomentou-se, ainda, a formação de novos pesquisadores na seara interdisciplinar entre o Direito e os vários

campos da tecnologia, notadamente o da ciência da informação, haja vista o expressivo número de graduandos que participaram efetivamente, com o devido protagonismo, das atividades.

A SKEMA Business School é entidade francesa sem fins lucrativos, com estrutura multicampi em cinco países de continentes diferentes (França, EUA, China, Brasil e África do Sul) e com três importantes acreditações internacionais (AMBA, EQUIS e AACSB), que demonstram sua vocação para pesquisa de excelência no universo da economia do conhecimento. A SKEMA acredita, mais do que nunca, que um mundo digital necessita de uma abordagem transdisciplinar.

Agradecemos a participação de todos neste grandioso evento e convidamos a comunidade científica a conhecer nossos projetos no campo do Direito e da tecnologia. Já está em funcionamento o projeto Nanodegrees, um conjunto de cursos práticos e avançados, de curta duração, acessíveis aos estudantes tanto de graduação, quanto de pós-graduação. Em breve, será lançada a pioneira pós-graduação lato sensu de Direito e Inteligência Artificial, com destacados professores da área. A SKEMA estrutura, ainda, um grupo de pesquisa em Direito e Inteligência Artificial e planeja o lançamento de um periódico científico sobre o tema.

Agradecemos ainda a todas as pesquisadoras e pesquisadores pela inestimável contribuição e desejamos a todos uma ótima e proveitosa leitura!

Belo Horizonte-MG, 09 de junho de 2021.

Profª. Drª. Geneviève Daniele Lucienne Dutrait Poulingue

Reitora – SKEMA Business School - Campus Belo Horizonte

Prof. Dr. Edgar Gastón Jacobs Flores Filho

Coordenador dos Projetos de Direito da SKEMA Business School

O USO DE ALGORITMOS DE RECONHECIMENTO FACIAL COMO AUXILIAR NA SEGURANÇA PÚBLICA

THE USE OF FACIAL RECOGNITION ALGORITHMS AS AN AID TO PUBLIC SECURITY

João Paulo Terra Silva
Leticia Rodrigues Clemente

Resumo

Na contemporaneidade, a aplicação de tecnologias para o reconhecimento facial é amplamente dispersa pela população, como em redes sociais e na segurança biométrica de bancos e aparelhos eletrônicos. Por outro lado, nota-se o crescente emprego desses algoritmos por órgãos de policiamento público, principalmente na prevenção de crimes e na captura de procurados e fugitivos. Portanto, o presente trabalho buscará analisar os riscos dessa manipulação sem o devido amparo jurídico, além da baixa confiabilidade dos sistemas de reconhecimento e, para tal, utilizou-se do método dedutivo, através da consulta de doutrinas, documentos e apontamentos de especialistas, além de análise de casos.

Palavras-chave: Direito penal, Segurança pública, Reconhecimento facial

Abstract/Resumen/Résumé

Nowadays, the application of technologies for facial recognition is widely dispersed among the population, as in social networks and in the biometric security of banks and electronic devices. However, there is a growing use of these algorithms by public policing bodies, mainly for preventing crimes and capturing the wanted and fugitives. Therefore, the present work will seek to analyze the risks of this manipulation without legal support, in addition to the low reliability of the recognition systems and, for this, it used the deductive method, through the consultation of doctrines, documents and notes of specialists, in addition to case analysis.

Keywords/Palabras-claves/Mots-clés: Criminal law, Public security, Facial recognition

INTRODUÇÃO

Hodiernamente, o uso de tecnologias que permitem o reconhecimento facial é amplamente difundido na sociedade, ao se estabelecer como um mecanismo empregado em diversos contextos, como nos *smartphones* e seus aplicativos, que permitem o desbloqueio e acesso por meio da leitura do rosto, substituindo as senhas numéricas e até a impressão digital. Contudo, diversos órgãos de segurança pública apreenderam que esse sistema pode ser empregado na busca de criminosos, crianças desaparecidas e, até mesmo, previsão e prevenção de delitos, mesmo que ao arrepio da lei.

Essa pesquisa debaterá sobre a limitação legal e tecnológica do uso de tecnologias de reconhecimento facial na segurança pública, e se justifica ao se constatar a rara legislação em relação ao tema, seu potencial para ofender direitos fundamentais, sua baixa eficiência e confiabilidade, além do custo econômico dos equipamentos para os órgãos públicos de policiamento.

O objetivo do estudo será a reflexão sobre a possibilidade de emprego dessas ferramentas como auxiliares na defesa social, apesar do atual encantamento digital. Tendo em consideração a atual escassez legislativa, tanto nacional quanto internacionalmente, seu uso antidemocrático por ordens políticas seria viabilizado. Além disso, no trabalho será considerado a baixa fiabilidade da inteligência artificial presentemente, não obstante seu alto custo financeiro para os órgãos públicos.

Dessa forma, a pesquisa utilizará o método dedutivo, com o estudo de doutrinas, documentos e artigos de especialistas, juntamente à análise de casos, com o intuito de debater a manipulação dos algoritmos de reconhecimento facial na segurança pública, expondo os riscos da busca pela amplificação da eficiência policial através do emprego dessas tecnologias para combater o crime nas grandes cidades.

1. O EMPREGO DE TECNOLOGIAS DE RECONHECIMENTO FACIAL COMO INSTRUMENTO COADJUVANTE NA SEGURANÇA PÚBLICA

Primordialmente, deve-se perceber que o reconhecimento facial é um dos mais populares sistemas de biometria, que se baseia nos traços faciais de cada indivíduo (PISA, 2012). Através de medidas entre os oitenta pontos nodais da face humana, tal como, a distância entre os olhos, o tamanho do queixo e o comprimento do nariz, é desenvolvido um banco de dados, que cria uma assinatura facial ímpar. Desse modo, no reconhecimento facial compara-se as características da imagem capturada no momento com as já inclusas nos arquivos, ou seja, com os padrões de faces pré-estabelecidos, com o objetivo de localizar o possuidor daquele rosto específico (PISA, 2012).

As implicações da utilização dessa tecnologia vão desde o entretenimento, como a marcação automática de amigos em fotos postadas em redes sociais, como o *Facebook* (FACEBOOK, 2021), até a substituição das senhas numéricas nos dispositivos (DA SILVA; DA SILVA, 2019). No entanto, diversos órgãos públicos perceberam o potencial que estes sistemas possuem de auxiliar no combate à criminalidade, em que pese o escasso arcabouço jurídico que sustente a utilização destes mecanismos, além da dificuldade que a legislação possui de escoltar o aprimoramento dos algoritmos.

Como por exemplo, em 2019, em uma tentativa de instalação de um sistema de reconhecimento facial no metrô de São Paulo - SP, houve a vinculação desse ao banco de dados da Secretaria de Segurança Pública, a fim de encontrar foragidos da Justiça. Como justificativa frisou-se a cooperação na busca de crianças perdidas nas estações de metrô, além da identificação de objetos suspeitos, auxiliando na segurança antiterrorista (TAUTE, 2020).

Entretanto, as críticas quanto ao uso dessa tecnologia em metrôs advêm da conjuntura de que, normalmente, não há uma crise de segurança que justifique a utilização dessas ferramentas, além dos custos econômicos, sociais e legais que exigem (TAUTE, 2020). Além disso, há inseguranças quanto a utilidade do mecanismo quando levado em conta o índice de desacertos que apresenta, como aconteceu em testes realizados no Rio de Janeiro - RJ: já no segundo dia, uma mulher foi erroneamente identificada como criminosa e levada à delegacia (WERNECK, 2019).

Ademais, em localidades como Praia Grande - SP, o algoritmo é amplamente usado com o objetivo de apontar pessoas procuradas pela Justiça, sendo alimentado por dados da própria Polícia Civil do município, com a previsão para expandir a aplicação em todo o estado. A justificativa para tal reside na diminuição dos índices de criminalidade na cidade, desde a implementação dessas ferramentas em locais estratégicos e em grandes eventos (DE MACEDO; JAVAROTTI; KIRITSCHENKO, 2019).

Outra utilidade para a aplicação dessa tecnologia pode ser percebida ao refletir sobre ataques terroristas em shows e multidões, em que a segurança comum nem sempre é suficiente, como já empregado nos espetáculos de diversos cantores (CANON, 2019). Por outro lado, também deve ser frisada a forma pela qual essa tecnologia pode ser utilizada, com potencial de ser mais prejudicial a certos grupos da sociedade. Por exemplo, no caso da aplicação no metrô de São Paulo, essa ferramenta poderia ser colocada contra ativistas políticos ou críticos das autoridades, por exemplo, compelindo-lhes a evitar essas áreas, de acordo com Taute, que salienta:

> Por tudo isso, o reconhecimento facial pode ser visto como ameaça à sociedade civil limitando o direito à privacidade, à liberdade de movimento, de reunião e associação. Este tipo de tecnologia pode dar a policiais em delegacias o poder de identificação de quem participa de protestos, comícios políticos, reuniões de igreja ou até dos Alcoólicos Anônimos.

Além disso, o mecanismo foi extensivamente utilizado para reprimir manifestantes em Hong Kong, em 2019, com propósito de controlar os protestantes contra o governo (PICHONELLI, 2021). Por isso, a manipulação desse sistema precisa ser uma polêmica constante em países democráticos (LAVADO, 2020).

No Brasil, o artigo 5º, *caput* e 6º, da Constituição Federal de 1988 institui a segurança pública como direito fundamental inviolável do ser humano e direito social de todos, além de que a garantia e manutenção da segurança pública é tida como dever do Estado, direito e responsabilidade de todos, devendo ser exercida à preservação da ordem pública e da incolumidade das pessoas e do patrimônio (BRASIL, 1988).

Nesse viés, se por um lado o reconhecimento facial se apresenta como uma interessante ferramenta para o enfrentamento da criminalidade, ao proporcionar uma sensação de segurança e vigilância constante, mais eficaz que rondas policiais comuns, a privação social do consentimento informado, isto é, não saber em quais momentos estão recorrendo ao dispositivo, nem a sua finalidade, exige ser ponderada nas tentativas brasileiras, com o objetivo de empregar a técnica para a segurança pública: se nãofor anunciada a justificativa da captura de dados e sua destinação, ou se as situações nas quais o povo é vigiado não forem sinalizadas, não há que se falar em aquiescência (DISPATCH, 2018).

No Brasil, o equipamento foi recorrentemente testado durante o Carnaval, o maior evento público do país, mas os resultados não foram animadores aos defensores desse mecanismo. Apesar de que em 2019, em Salvador - BA, um homem procurado desde 2017 por homicídio foi preso após ser reconhecido pelo aparelho, mesmo fantasiado de mulher (LAVADO, 2020), no Rio de Janeiro - RJ, o índice de erro do sistema testado foi de 90%, de acordo com a organização *Coding Rights* (TAUTE, 2020). Com isso, transparece a assustadora realidade: se grande parte das correspondências forem falsos positivos, automaticamente um inocente será tido como suspeito pela polícia.

Essa preocupação já é notada em mudanças como em relação à venda às forças policiais de equipamentos para reconhecimento facial por empresas como *Amazon* e *Microsoft*, ainda em 2020. Nesse caso, as empresas se comprometeram a não vender seus mecanismos ao governo, enquanto não houver novas leis específicas sobre seu emprego no combate ao crime, destacando o potencial abuso das ferramentas (BURGESS, 2020). Essa modificação teve início

a partir da onda de protestos contra a brutalidade policial e racismo, após o assassinato de George Floyd.

Nessa senda, é fundamental salientar os dois tópicos a serem abordados ao se tratar sobre as tecnologias de reconhecimento facial na segurança pública: as adversidades jurídicas do equipamento, que surgem ao empregá-lo para o combate ao crime e as complicações técnicas do mesmo, no que tange à precisão do algoritmo (LAVADO, 2020).

De início, reforça-se que manipular o mecanismo para impedir crimes se mostra uma responsabilidade complexa, comparável ao pensamento de Cesare Lombroso e sua primitiva teoria do criminoso nato, que defendia a segregação social preventiva de certos indivíduos, baseada no formato de rosto e outras medidas corporais (FERNANDES, 2018), sendo um sistema de repressão social disfarçada de auxílio à segurança pública, como na atual e questionável ideia de policiamento preditivo (BURGESS, 2018).

Além disso, nota-se, igualmente, que a privação do consentimento informado, por parte da população, resulta em graves problemas éticos e legais, já que, ao tirar do cidadão o poder de escolha em ter sua imagem captada ou não, converte-se em uma imposição governamental, com o pretexto de coadjuvar no combate ao crime (DISPATCH, 2018).

Por esse motivo, é necessário que estejam bem definidas as situações em que o mecanismo será empregado, visto que restringem direitos fundamentais dos indivíduos. Com isso, é certo que uma tecnovigilância dessa grandeza sem dúvida afeta a vida privada e a intimidade de cada cidadão (PRADO, 2020), não apenas os suspeitos e procurados pela polícia.

CONSIDERAÇÕES FINAIS

Em suma, atualmente é percebida a insuficiente transparência por parte dos órgãos públicos quanto ao método de reconhecimento facial adotado, sua finalidade e eficiência. Esses fatores viabilizam a intensificação do encarceramento em massa de minorias e da falsa recognição de procurados e foragidos, repercutindo na consolidação de preconceitos automatizados. Nesses embates é onde se encontra a importância desse trabalho e do debate sobre o consumo dessa técnica na segurança pública.

No que tange à baixa regulamentação legal sobre o seu emprego, foi notado que os sistemas de reconhecimento facial devem estar adequados e delimitados pelos direitos fundamentais e pelas regras processuais-penais, além de que sua utilização deve ser restringida durante o tempo em que não forem elaboradas legislações especiais, que assegurem ao indivíduo seu direito ao consentimento informado antes de ter suas informações faciais capturadas e processadas. Assim, caberá ao Poder Legislativo coibir os excessos originados do encantamento digital, além da indispensabilidade de democratizar os debates sobre o tema e

suas consequentes adversidades, tornando-o tão público quanto a ferramenta em si, ao encorajar a participação popular em diálogos com órgãos governamentais de segurança pública.

Em virtude disso, deve-se questionar, igualmente, a real necessidade do consumo de tecnologias de reconhecimento facial para o combate ao crime, tendo em vista seu alto custo, tanto jurídico quanto econômico - já que os órgãos de segurança pública deverão ponderar sobre o orçamento disponível para investimentos do tipo, refletindo em uma alteração na forma pela qual o dinheiro será distribuído nessa área, pela demanda por melhor aparato tecnológico em todas as regiões do país. Por fim, a evidência concebida pelas análises quanto essa aplicação demonstra que os resultados não fazem jus ao tempo e recursos exigidos por esse equipamento, além da inquietante ameaça de violação dos direitos fundamentais.

REFERÊNCIAS

BIG BROTHER WATCH. **The Lawless Growth of Facial Recognition in UK policing**. **Big Brother Watch**. 2018. Disponível em: https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/report. Acesso em: 25 nov. 2020.

BRASIL. Constituição da República Federativa do Brasil de 1988. **Diário Oficial da União**, 05 de outubro de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 11 jan. 2021.

CANON, Gabrielle. **How Taylor Swift showed us the scary future of facial recognition Facial recognition. The Guardian**. 2019. Disponível em: https://www.theguardian.com/technology/2019/feb/15/how-taylor-swift-showed-us-the-scaryfuture-of-facial-recognition. Acesso em: 5 nov. 2020.

DA SILVA, Rosane Leal; DA SILVA, Fernanda dos Santos Rodrigues. Reconhecimento facial e segurança pública: Os perigos do uso da tecnologia no sistema penal seletivo brasileiro. In: 5º CONGRESSO INTERNACIONAL DE DIREITO E CONTEMPORANEIDADE: MÍDIAS E DIREITOS DA SOCIEDADE EM REDE. 2019. **Anais eletrônicos [...]** Santa Maria - RS, 2019. Disponível em: https://www.ufsm.br/app/uploads/sites/563/2019/09/5.23.pdf. Acesso em: 24 dez. 2020.

DE MACEDO, Wagner Lucas Rodrigues; JAVAROTTI, Marcos Ricardo Castilho; KIRITSCHENKO, Ana Carolina Barbosa. **Tecnologia de reconhecimento facial e discriminação**. **Consultor Jurídico**. 2019. Disponível em: https://www.conjur.com.br/2019-ago-28/opiniao-tecnologia-reconhecimento-facial-discriminacao#:~:text=Verifica%2Dse%2C%20portanto%2C%20que,raz%C3%A3o%20de%20suas%20atuais%20limita%C3%A7%C3%B5es. Acesso em: 12 nov. 2020.

DISPATCH, Zhengzhou. **Looking Through the Eyes of China's Surveillance State. The New York Times.** 2018. Disponível em:

https://www.nytimes.com/2018/07/16/technology/china-surveillance-state.html. Acesso em: 26 nov. 2020.

FACEBOOK. **O que é a configuração de reconhecimento facial no Facebook e como ela funciona?**. Disponível em: https://pt-br.facebook.com/help/122175507864081. Acesso em: 17 nov. 2020.

FERNANDES, Bianca da Silva. Cesare Lombroso e a teoria do criminoso nato. 2018. Disponível em: https://canalcienciascriminais.jusbrasil.com.br/artigos/625021486/cesare-lombroso-e-a-teoria-do-criminoso-nato. Acesso em: 19 de abr. de 2021.

LAVADO, Thiago. **Aumento do uso de reconhecimento facial pelo poder público no Brasil levanta debate sobre limites da tecnologia**. **G1**. 2020. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2020/02/21/aumento-do-uso-de-reconhecimento-facial-pelo-poder-publico-no-brasil-levanta-debate-sobre-limites-da-tecnologia.ghtml. Acesso em: 8 jan. 2021.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software**. **NIST**. 2020. Disponível em: https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software. Acesso em: 6 jan. 2021.

PICHONELLI, Matheus. **Seriam as manifestações de Hong Kong as mais distópicas já realizadas?. UOL**. 2019. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2019/10/11/seriam-as-manifestacoes-de-hong-kong-as-mais-distopicas-ja-realizadas.htm. Acesso em: 19 abr. 2021.

PISA, Pedro. **Como funciona o reconhecimento facial**. **TechTudo**. 2012. Disponível em: https://www.techtudo.com.br/artigos/noticia/2012/04/como-funciona-o-reconhecimento-facial.html. Acesso em: 9 dez. 2020.

PORTER, Tony. **Surveillance Camera Commissioner's annual report**. **Gov.UK**. 2017. Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/772440/CCS207_CCS1218140748-001_SCC_AR_2017-18_Web_Accessible.pdf. Acesso em: 6 jan. 2021.

PRADO, Geraldo. **Dados, prova digital e devido processo penal**. **Consultor Jurídico**. 2020. Disponível em: https://www.conjur.com.br/2020-ago-26/geraldo-prado-dados-prova-digital-devido-processo-penal-parte-iii. Acesso em: 16 dez. 2020.

PRETALAB. **Um levantamento sobre a necessidade e a pertinência de incluir mais mulheres negras na inovação e na tecnologia**. **Pretalab**. 2018. Disponível em: https://www.pretalab.com. Acesso em: 11 jan. 2021.

ROTH, Lorna. **Questão de Pele**. **Revisa Zum**. 2016. Disponível em: https://revistazum.com.br/revista-zum-10/questao-de-pele. Acesso em: 21 dez. 2020.

TAUTE, Fabian. **Reconhecimento Facial e suas controvérsias**. **Heinrich-Böll-Stiftung**. 2020. Disponível em: https://br.boell.org/pt-br/2020/02/05/reconhecimento-facial-e-suas-controversias. Acesso em: 8 dez. 2020.

WERNECK, Antônio. **Reconhecimento facial falha em segundo dia, e mulher inocente é confundida com criminosa já presa. O Globo**. 2016. Disponível em: https://oglobo.globo.com/rio/reconhecimento-facial-falha-em-segundo-dia-mulher-inocente-confundida-com-criminosa-ja-presa-23798913. Acesso em: 19 abr. 2021.

WOOD, Collin. **New York bans facial recognition in schools until at least 2022**. **EdScoop**. 2020. Disponível em: https://edscoop.com/new-york-facial-recognition-ban. Acesso em: 8 jan. 2021.