RCi
Revista Científica Integrada

Considerações acerca do uso de tecnologias de reconhecimento facial como instrumento de segurança pública

Considerations about the use of facial recognition technologies as a public safety tool

José Roberto Macri Júnior[1] | https://orcid.org/0000-0003-2021-3524
Bianka Jaquetti Macri[1] | https://orcid.org/0000-0002-8438-5993
Helena Frontini[1] | https://orcid.org/0009-0007-5027-1203

Artigo de revisão

Como Citar
Macri Júnior JR, Macri BJ, Frontini H. Considerações acerca do uso de tecnologias de reconhecimento facial como instrumento de segurança pública. Rev Científica Integrada 2023, 6(1):e202320. DOI: https://doi.org/10.59464/2359-4632.2023.3102

Conflito de interesses
Não há conflito de interesses.

Submetido em: 12/04/2023
Aceito em: 17/08/2023
Publicado em: 01/09/2023

[1]Universidade de Ribeirão Preto. Ribeirão Preto, São Paulo, Brasil.

Autor correspondente
José Roberto Macri Júnior
Av. Costábile Romano, 2201 - Nova Ribeirânia, Ribeirão Preto, São Paulo, Brasil.
E-mail: macrijunior@hotmail.com

Revista Científica Integrada (ISSN 2359-4632)
https://revistas.unaerp.br/rci

RESUMO

Objetivo: Analisar como a emergência das tecnologias de reconhecimento facial podem impactar direitos fundamentais, notadamente nas hipóteses em que os algoritmos de reconhecimento são aplicados no âmbito da segurança pública. **Métodos:** Trata-se de uma revisão narrativa, realizada entre os meses de janeiro e março de 2023. Utilizou-se a base eletrônica Hein Online. O termo de busca utilizado foi "facial recognition technologies". Foram selecionados tão-somente publicações classificadas como artigos – desde que abordassem a temática do funcionamento ou da aplicação das tecnologias de reconhecimento facial –, excluindo-se outras produções (comentários legislativos, jurisprudência comentada etc.). Os trabalhos deveriam responder: como funcionam as tecnologias de reconhecimento facial? como esta tecnologia pode ser aplicada como instrumento de segurança pública e quais os riscos envolvidos? em razão dos riscos, quais as propostas para evitar que a aplicação da tecnologia resulte em violações de direitos? **Resultados:** Apresenta-se a proposta de suspensão do uso dos algoritmos de reconhecimento até que sejam supridas deficiências técnicas e regulatórias. A ideia de uma moratória, todavia, enfrenta a resistência de um contexto político-criminal caracterizado por crescentes demandas por segurança via expansão dos meios repressivos. **Conclusão:** Deve-se procurar regulamentar o uso das tecnologias de reconhecimento facial, o qual deve pautar-se, especialmente em razão de eventuais falhas técnicas, nos juízos de proporcionalidade e necessidade.
Palavras-chave: Tecnologias de reconhecimento facial; Segurança pública; Direitos fundamentais.

ABSTRACT

Objective: To analyze how the emergence of facial recognition technologies can impact fundamental rights, notably in cases where recognition algorithms are applied in the context of public safety. **Methods**: This is a narrative review, carried out between January and March 2023. The electronic database Hein Online was used. The search term used was "facial recognition technologies". Only publications classified as articles were selected – if they addressed the theme of the operation or application of facial recognition technologies –, excluding other productions (legislative comments, commented jurisprudence, etc.). Papers should answer: how do facial recognition technologies work? how can this technology be applied as a public safety tool and what are the risks involved? given the risks, what are the proposals to prevent the application of technology from resulting in violations of rights? **Results**: A proposal is presented to suspend the use of recognition algorithms until technical and regulatory deficiencies are corrected. The idea of a moratorium, however, faces resistance from a political-criminal context characterized by growing demands for security through the expansion of repressive means. **Conclusion**: The use of facial recognition technologies should be regulated, which should be based, especially in view of possible technical failures, on judgments of proportionality and necessity.
Keywords: Facial recognition technologies; Public security; Fundamental rights.

Introdução

As tecnologias de reconhecimento facial têm demonstrado uma crescente variedade de possíveis aplicações. A utilização de tais tecnologias no âmbito privado revela suas potencialidades comerciais e econômicas. Já no âmbito estatal, as tecnologias de reconhecimento podem ser utilizadas como instrumento de segurança pública, seja por meio da vigilância preventiva, seja como forma de aumentar a efetividade da persecução penal (O'FLAHERTY, 2020; ROWE, 2020).

A adoção da tecnologia, notadamente por órgãos estatais, desperta uma série de inquietações relativas à proteção de direitos fundamentais. De fato, a captação não consensual de imagens e a possibilidade de falhas técnicas – especialmente diante da constatação de que estas falhas são mais comuns em peles mais escuras – são exemplos de situações que colocam em xeque a adequação do emprego das tecnologias de reconhecimento em vista da inviolabilidade de direitos fundamentais (O'FLAHERTY, 2020; SIMONITIS, 2021; ANIULIS, 2022).

Este trabalho pretende apresentar o estado da discussão acerca do emprego de tecnologias de reconhecimento facial como instrumento de segurança pública. Objetiva-se em um primeiro momento, compreender como funcionam as tecnologias de reconhecimento facial, a fim de identificar os riscos de sua aplicação. Em seguida, em face dos riscos identificados, será possível compreender os fundamentos das duas principais correntes de recomendações acerca da aplicabilidade da tecnologia de reconhecimento no âmbito da segurança pública, a saber: a proposta de moratória – isto é, de suspensão de uso da tecnologia até que limitações técnicas e regulatórias sejam sanadas –, bem como as recomendações internacionais que procuram conciliar, de uma lado, o emprego das tecnologias de reconhecimento como instrumento de garantia de segurança, com, de outro, a inviolabilidade de direitos fundamentais.

Métodos

Trata-se de uma revisão narrativa da literatura sobre tecnologia de reconhecimento facial e segurança pública, realizada entre os meses de janeiro e março de 2023. Os autores fizeram o levantamento bibliográfico por meio da base eletrônica HeinOnline, embora tenham sido consultadas outras fontes sobre temas correlatos, por exemplo, privacidade, terrorismo e expansão penal. O termo de busca utilizado foi “facial recognition technologies”. Sendo tema relativamente novo, não foi realizado um recorte temporal para seleção de artigos; contudo, observa-se que a quase totalidade dos textos específicos sobre reconhecimento facial são posteriores a 2019. Foram selecionados tão-somente publicações classificadas como artigos – desde que abordassem a temática do funcionamento ou da aplicação das tecnologias de reconhecimento facial –, excluindo-se outras produções (comentários legislativos, jurisprudência comentada etc.).

Os trabalhos selecionados foram analisados de modo a poder responder as seguintes questões: como funcionam as tecnologias de reconhecimento facial; como esta tecnologia pode ser aplicada como instrumento de segurança pública e quais os riscos envolvidos; em razão dos riscos, quais as propostas para evitar que a aplicação da tecnologia resulte em violações de direitos.

Resultados e discussão

Tecnologia de reconhecimento facial: funcionamento, aplicações e riscos

O princípio fundamental por trás do desenvolvimento de tecnologias de reconhecimento facial é o de que a disposição de diversos traços faciais cria uma espécie de identidade única para cada rosto. As distâncias entre pontos específicos da face (e.g., a profundidade dos olhos, largura do nariz, formato do queixo e das mandíbulas etc.) podem ser mensuradas, e algoritmos de reconhecimento facial podem usar tais medidas para comparar rostos (WIEHL, 2013). Dessa forma, a tecnologia de reconhecimento facial pretende determinar, por meio de comparação, se duas imagens pertencem ao mesmo rosto, isto é, se duas captações faciais são da mesma pessoa (O'FLAHERTY, 2020). Referida “comparação” consiste no processamento de imagens faciais para fins de (I) verificação, quando duas imagens faciais são comparadas para verificar se elas pertencem ao mesmo indivíduo, ou de (II) identificação, quando uma imagem facial é enviada a uma base de dados de imagens para que se descubra a identidade da pessoa cuja imagem está sendo captada (O'FLAHERTY, 2020; ANIULIS, 2022).

O acelerado desenvolvimento da Inteligência Artificial tem melhorado consideravelmente a precisão das tecnologias de reconhecimento facial, tornando-as atrativas, tanto para o setor privado quanto para o setor público (O'FLAHERTY, 2020). Com efeito, o reconhecimento facial já é uma realidade cotidiana, é certo que em graus diversos, em muitos

países. De compras a transferências bancárias, de redes sociais a ingresso em edifícios, são muito variados os usos das tecnologias de reconhecimento facial adotados por agentes privados (ROWE, 2020).

E diversos estudos indicam que as possibilidades de uso podem aumentar de maneira significativa, especialmente com o desenvolvimento de tecnologias que, para além do reconhecimento, conseguem "interpretar" a face de uma pessoa: Bala (2020) aponta que a tecnologia já é empregada em escolas chinesas para medir o nível de atenção dos estudantes durante as aulas, o que poderia ter efeitos na formação das crianças, por exemplo, acostumando-as à vigilância constante; Wilkinson (2021) noticia que há algoritmos que detectam – com alto grau de precisão – a orientação sexual de uma pessoa por meio da análise de seu rosto; Dixon, Kiazim, Creed e Bowden (2021) destacam o uso da tecnologia no ambiente de trabalho, não só como forma de controle de concentração nas atividades, mas também no momento da contratação, como uma forma de atribuir notas de "empregabilidade" a partir da análise da personalidade; Rowe (2020) informa que o setor privado tem adotado a tecnologia para avaliar o estado geral de saúde das pessoas, bem como, por meio da captação de "movimentos faciais suspeitos", determinar o nível de honestidade de pessoas, o que seria uma informação importante, por exemplo, para concessão de crédito.

No âmbito estatal, acredita-se que, no futuro, serão desenvolvidos algoritmos que pretendem indicar a probabilidade de alguém cometer um ato terrorista, ou delinquir de alguma outra maneira (MARTIN, 2020). Contemporaneamente, a tecnologia de reconhecimento tem sido usada como instrumento de segurança pública, seja como forma de prevenção de delitos (por exemplo, vigilância de aeroportos para detecção de possíveis atos terroristas), seja como instrumento para maior efetividade de persecução penal (O'FLAHERTY, 2020; ROWE, 2020).

A adoção das tecnologias de reconhecimento facial por parte de órgãos estatais tem potencial de afetar, em intensidades variadas, diversos direitos fundamentais – sendo o exemplo mais evidente a privacidade –, seja em razão do próprio uso da tecnologia, seja em razão de ainda existentes limitações técnicas dos sistemas de comparação e processamento de imagens (O'FLAHERTY, 2020). Efetivamente, nas hipóteses de perfeito funcionamento técnico, a dignidade humana, globalmente considerada, pode ser afetada, na medida em que não há consentimento ou possibilidade de recusa para a captação dos dados pessoais (O'FLAHERTY, 2020), independentemente de, por exemplo, existir alguma objeção de ordem religiosa por parte da pessoa cuja imagem é coletada (ROWE, 2020). E, precisamente em razão dessa forma involuntária de captação de dados, a tecnologia de reconhecimento facial afeta indiretamente as liberdades de reunião e de expressão. O mero receio de estar sendo vigiado e facilmente identificado cria uma série de bloqueios para as livres manifestações. Em outros termos, a tecnologia de reconhecimento estimula certa autocensura, o que impacta o direito à livre manifestação do pensamento. Como bem sintetizaram Hamann e Smith (2019, p.13), o "chilling effect" provoca a "self-censorship".

A adoção de tecnologias de reconhecimento pode ter efeitos ainda mais sérios a longo prazo. Nesse sentido, Bala (2020), ao estudar os possíveis impactos que a vigilância eletrônica pode causar no ambiente escolar, afirma ser o monitoramento da aprendizagem infantil um caminho para a deterioração do que se conhece como sociedade livre, pois a vigilância incessante passaria a ser naturalizada pelas futuras gerações. No limite, a vigilância em massa, a longo prazo, pode afetar o funcionamento da democracia, visto ser a privacidade um conceito central às sociedades plurais (O'FLAHERTY, 2020; RODRÍGUEZ, 2008).

Embora o perfeito funcionamento das tecnologias de reconhecimento tenha impactos nos direitos fundamentais, estes são mais diretamente afetados pelas limitações ou mau funcionamento da tecnologia. De fato, apesar do desenvolvimento recente, as tecnologias de reconhecimento facial estão longe da indefectibilidade (SIMONITIS, 2021). Os riscos de "mismatching", isto é, reconhecimentos errôneos, são muito maiores no processamento de imagens para fins de identificação do que para fins de verificação (ANIULIS, 2022), visto que, em geral, as imagens processadas para identificar um rosto são captadas em ambientes não controlados (HAMANN; SMITH, 2019), de modo que a imagem – especialmente se captada em movimento – não atinge um padrão de qualidade que eliminaria ou reduziria significativamente a probabilidade de erro no reconhecimento (SIMONITIS, 2021). Outrossim, o processo de reconhecimento facial pode falhar em razão de mudanças naturais na face humana: variação da massa corporal, corte de cabelo, crescimento ou retirada de barba, além das alterações faciais decorrentes do envelhecimento (HAMANN; SMITH, 2019; SIMONITIS, 2021).

Os erros de reconhecimento facial causam ainda maiores preocupações, do ponto de vista dos direitos fundamentais, quando se constata que a precisão do

reconhecimento diminui para pessoas que não são homens brancos (O'FLAHERTY, 2020). Com efeito, os índices de falsos positivos são maiores para não caucasianos, e, de modo geral, as tecnologias são mais imprecisas para reconhecer rostos femininos, o que faz com que uma mulher de pele escura tenha maior probabilidade de ser incorretamente identificada do que um homem de pele clara (HAMANN; SMITH, 2019; O'FLAHERTY, 2020; SIMONITIS, 2021; ANIULIS, 2022). A imprecisão variável de acordo com a cor da pele pode resultar em discriminação, notadamente nas circunstâncias em que o Estado utiliza a tecnologia de reconhecimento como ferramenta de segurança pública (O'FLAHERTY, 2020). Por essas razões, há recomendações de que os grandes consumidores da tecnologia de reconhecimento (em especial, o Estado por meio do aparato de segurança pública) exijam dos desenvolvedores tecnológicos ajustes nas codificações (MARTIN, 2020).

Argumenta-se, por outro lado, que a discriminação não é um efeito colateral das limitações técnicas, mas sim o resultado previsível de práticas discriminatórias antecedentes ao uso da tecnologia de reconhecimento (ANIULIS, 2022). Nesse sentido, o processo discriminatório teria início já no treinamento do algoritmo, procedimento no qual haveria predominância de imagens de homens brancos. Além disso, os vieses da tecnologia se manifestariam com sua aplicação às listas de vigilância ("watchlists"), desenvolvidas a partir de bases de dados policiais, as quais já apresentam sensíveis disparidades em termos étnicos. Tal enviesamento não pode ser superado simplesmente com o aperfeiçoamento tecnológico (ANIULIS, 2022).

Em vista de possíveis efeitos deletérios decorrentes do uso da emergente tecnologia, há propostas para suspensão de sua utilização, notadamente quanto ao emprego por órgãos de segurança pública. De fato, defensores de uma moratória afirmam que, em vista de limitações técnicas e dos vieses inerentes aos softwares (em razão, como já mencionado, de sua programação), a tecnologia de reconhecimento facial não pode ser um instrumento utilizado no dia a dia pelas forças de segurança. Chega-se a propor uma ampla suspensão até que, após a discussão de especialistas de diversas áreas, a tecnologia seja regulamentada de forma a não violar direitos fundamentais (MARTIN, 2020). Em síntese, nesse ínterim, a tecnologia deveria ser compreendida, aperfeiçoada e adequadamente regulamentada (ROWE, 2020).

Entretanto, contra a prudência da proposta de moratória, há que se considerar o enorme potencial de natureza econômica da tecnologia de reconhecimento, o qual, por si só, poderia ser suficiente para garantir a permanência da tecnologia no cotidiano (SIMONITIS, 2021). E, também, não parece provável que as forças de segurança não utilizem tecnologia de ponta para tentar garantir a paz social (SIMONITIS, 2021). Com efeito, o contexto político-criminal das últimas décadas é o de recrudescimento punitivo motivado por crescentes demandas sociais por segurança (MENDONZA BUERGO, 2001). De fato, há uma série de pressões de vários grupos sociais para que as leis penais "modernizem-se", tornando-se mais aptas a regular situações (potencialmente) conflitivas (DÍEZ RIPOLLÉS, 2005). Embora se possa objetar que o juízo de adequação em relação às novas leis repressivas não seja completamente racional, visto que as demandas por proteção via punitiva nascem de um contexto de fortalecimento de medos sociais (GLASSNER, 2009; PASTANA, 2003; VOZMEDIANO, 2008), permanece o fato de que os meios de repressão se expandem, mesmo que irracionalmente (HUSAK, 2008).

A luta contra o terrorismo – na qual mesmo os defensores de um uso parcimonioso das tecnologias de reconhecimento facial admitem seu emprego (O'FLAHERTY, 2020) – é uma espécie de paradigma do inflacionamento penal: o combate ao terrorismo combina – quase em uma autonegação do Estado de Direito (CANO PAÑOS, 2011) – punições severas com flexibilizações de regras de imputação e de garantias fundamentais (SILVA SÁNCHEZ, 2001). O combate ao terrorismo funciona como máxima ilustração de como os impactos em direitos fundamentais são considerados – ao menos por parte da sociedade – aceitáveis desde que a contraprestação seja a proteção contra delitos graves. As tecnologias de reconhecimento facial aparecem precisamente nesse contexto em que, político-criminalmente, transaciona-se liberdade por segurança.

O contexto de crescente demanda por proteção via repressiva acaba por, no limite, tornar aceitável uma inversão da máxima do in dubio pro reo. Os falsos reconhecimentos positivos seriam um preço razoável a se pagar pela sensação de segurança e pela efetividade do controle dos índices de criminalidade. Com base em ampla bibliografia da área da Psicologia, Brownsword e Harel (2019, p.110) afirmam que a maior preocupação com a não punição do culpado do que com a punição injusta do inocente decorre da "aversão ao arrependimento" ("regret aversion"): um falso negativo (i.e., a liberação de alguém que cometeu um crime) seria socialmente considerado mais grave do que um falso positivo – o

que implicaria algum tipo de sanção ou constrangimento a uma pessoa inocente –, pois liberar alguém que comete crimes seria mais danoso do que não liberar alguém que poderia ou não eventualmente delinquir.

Possibilidade de um uso proporcional da tecnologia de reconhecimento facial

A adoção das tecnologias de reconhecimento facial constituem uma ameaça aos direitos fundamentais, seja em razão da possibilidade de uso indevido ou processamento incorreto de dados pessoais coletados, seja em virtude de eventuais falhas técnicas. Entretanto, a violação de direitos fundamentais não é a consequência inevitável da utilização das tecnologias de reconhecimento. Com efeito, diversas medidas podem ser tomadas para que o uso da tecnologia de reconhecimento não implique lesão a direitos (O'FLAHERTY, 2020; SIMONITIS, 2021). Nesse sentido, há diversas propostas que procuram delinear o que seria um uso proporcional das tecnologias de reconhecimento facial, isto é, um uso que concilie a busca por segurança com a inviolabilidade de certos direitos.

Primeiramente, recomenda-se que os Estados elaborem uma detalhada regulamentação da aplicação das tecnologias de reconhecimento. Deve-se estabelecer que a determinação de quando o processamento de imagens faciais será necessário e proporcional dependerá do propósito pelo qual a tecnologia será usada. Assim, formas de reconhecimento facial que envolvam muita intrusão em direitos fundamentais, comprometendo o núcleo inviolável de um ou mais desses direitos, será ilícito (O'FLAHERTY, 2020).

Em segundo lugar, recomenda-se que a regulamentação e, consequentemente, a aplicação das tecnologias levem em conta a distinção entre processamento de imagens faciais para fins de verificação ou para fins de identificação, visto que o risco de interferências em direitos fundamentais é maior no segundo caso, de modo que se deve verificar com maior rigor os critérios de necessidade e proporcionalidade (O'FLAHERTY, 2020; ANIULIS, 2022).

Em terceiro lugar, não se pode ignorar que as chamadas “live facial recognition technologies” são particularmente problemáticas em termos de riscos a direitos fundamentais. De fato, o uso dessas tecnologias desperta sentimentos diversos na população e levanta temores de um significativo desequilíbrio de poder entre o Estado e o indivíduo. Tendo em vista que o cidadão pode não estar ciente de que sua imagem facial está sendo comparada às imagens de uma base de dados, e considerando que a captura ao vivo tem um maior índice de erro do que a captura de imagens faciais em ambientes controlados (HAMANN; SMITH, 2019; SIMONITIS, 2021), o uso dessas imagens deve ser bastante excepcional. Recomenda-se a restrição de seu uso apenas para o combate ao terrorismo e outras formas de crimes graves, ou para identificação de pessoas desaparecidas ou vítimas de crimes (O'FLAHERTY, 2020).

Em quarto lugar, em razão das mencionadas limitações técnicas, é imprescindível que os resultados fornecidos por algoritmos de tecnologia de reconhecimento facial sejam concebidos apenas como a indicação de (relativamente alta) probabilidade de que duas imagens sejam da mesma pessoa. A margem de erro da tecnologia deve implicar um reforço ao tratamento digno dispensado ao suspeito (O'FLAHERTY, 2020). Ademais, o reconhecimento realizado por softwares não pode constituir, por si só, fundamento legítimo para a restrição da liberdade. Não obstante, pode ser utilizado como instrumento para levantamento de outras linhas de investigação, bem como é possível que o reconhecimento por algoritmo integre um conjunto probatório mais robusto (HAMANN; SMITH, 2019).

Por fim, faz-se necessária uma avaliação de impacto dos direitos fundamentais em razão da aplicação das tecnologias de reconhecimento facial, qualquer que seja o contexto de uso. Esta avaliação requer que as autoridades públicas obtenham dos desenvolvedores todas as informações necessárias para a análise de impacto. Consequentemente, conceitos como confidencialidade e segredos comerciais devem ser interpretados à luz das necessidades de preservação de direitos fundamentais (O'FLAHERTY, 2020). Outrossim, os órgãos de segurança devem exigir dos desenvolvedores tecnológicos que considerações acerca de direitos fundamentais estejam inseridas nas especificações técnicas, em especial: proteção de dados e requisitos não-discriminatórios (O'FLAHERTY, 2020; MARTIN, 2020).

Conclusão

As tecnologias de reconhecimento facial podem afetar diversos direitos fundamentais. De fato, o perfeito funcionamento dos softwares de reconhecimento tem um considerável potencial de inibir livres manifestações públicas, estimulando, em certa medida, a autocensura. Nas hipóteses de

funcionamento incorreto da tecnologia de reconhecimento, direitos fundamentais ficam em maior risco, especialmente diante da possibilidade de falsos positivos, isto é, identificações errôneas, as quais são consideravelmente mais comuns para pessoas de pele mais escura.

Em vista da defectibilidade da tecnologia, há propostas de uma moratória. A suspensão do uso da tecnologia, entretanto, parece improvável. O contexto político-criminal contemporâneo caracteriza-se pela demanda por segurança via desenvolvimento de instrumentos repressivos, ainda que isto implique flexibilizações de direitos e garantias. Dessa forma, sendo pouco crível a moratória, deve-se procurar regulamentar o uso das tecnologias de reconhecimento facial, o qual deve pautar-se, especialmente em razão de eventuais falhas técnicas, nos juízos de proporcionalidade e necessidade.

Referências

ANIULIS, Harry. Facial Recognition Technology, Privacy and Administrative Law. **University of New South Wales Law Journal**. vol.45, n.4, 2022.

BALA, Nila. The danger of facial recognition in our children's classrooms. **Duke Law & Technology Review**. vol.18, 2020.

BROWNSWORD, Roger; HAREL, Alon. Law, liberty and technology: criminal justice in the context of smart machines. **International Journal of Law in Context**. vol.15, 2019.

CANO PAÑOS, Miguel Ángel. La 'guerra contra el terrorismo' en Alemania. **Análisis histórico-jurídico de la legislación penal y procesal**. In: MAIER, Julio B. J. et al. (Directores). Dogmática penal entre naturalismo y normativismo. Libro en homenaje a Eberhard Struensee. Buenos Aires: Ad-Hoc, 2011.

DÍEZ RIPOLLÉS, José Luis. **A racionalidade das leis penais**. Teoria e prática. Trad. Luiz Regis Prado. São Paulo: Revista dos Tribunais, 2005.

DIXON, Alison; KIAZIM, Oran; CREED, Stephanie; BOWDEN, Olivia. Facial Recognition Technology in Employment: What You Need to Know. **The Journal of Robotics, Artificial Intelligence & Law**. vol.4, 2021.

GLASSNER, Barry. **The culture of fear**. New York: Basic Books, 2009.

HAMANN, Kristine; SMITH, Rachel. Facial Recognition Technology: Where Will It Take Us. **Criminal Justice**. vol.34, n.1, 2019.

HUSAK, Douglas. **Overcriminalization**. The limits of the criminal law. New York: Oxford University Press, 2008.

MARTIN, Cameron. Facial Recognition in Law Enforcement. **Seattle Journal for Social Justice**. vol.19, n.1, 2020.

MENDONZA BUERGO, Blanca. **El derecho penal en la sociedad del riesgo**. Madrid, Civitas, 2001.

O'FLAHERTY, Michael. Facial Recognition Technology and Fundamental Rights. **European Data Protection Law Review**. vol.6, n.2, 2020.

PASTANA, Débora Regina. **Cultura do medo**: reflexões sobre violência criminal, controle social e cidadania no Brasil. São Paulo: IBCCRIM, 2003.

RODRÍGUEZ, Víctor Gabriel. **Tutela penal da intimidade**. Perspectivas da atuação penal na sociedade da informação. São Paulo: Editora Atlas, 2008.

ROWE, Elizabeth A. Regulating facial recognition technology in the private sector. **Stanford Technology Law Review**. vol.24, n.1, 2020.

SILVA SÁNCHEZ, Jesús-María. **La expansión del derecho penal**: aspectos de la política criminal en las sociedades postindustriales. 2.ed. Madrid: Civitas, 2001.

SIMONITIS, Mark. Facial Recognition Technology and the Constitution. **Notre Dame Journal on Emerging Technologies**. vol.2, n.2, 2021.

VOZMEDIANO, Laura, et al. Problemas de medición del miedo al delito: Algunas respuestas teóricas y técnicas. **Revista Electrónica de Ciencia Penal y Criminología (en línea)**. p. 10-07, 2008.

WIEHL, Tom. Human and Computerized Facial Recognition: Comparison and Constitutional Analysis. **Northwestern Interdisciplinary Law Review**. vol.6, 2013.

WILKINSON, Phillip H. C. The Legal Implications of Sexual Orientation-Detecting Facial Recognition Technology. **Dukeminier Awards**: Best Sexual

Orientation and Gender Identity Law Review. vol.20, 2021.

Contribuições dos autores

Macri Júnior JR foi responsável pela concepção e redação do artigo; Macri BJ foi responsável pela revisão crítica relevante do conteúdo intelectual; Frontini H foi responsável pela aprovação final da versão a ser publicada.

Editor-chefe
José Claudio Garcia Lira Neto