INTERFACE TECNOLÓGICA

TECNOLOGIA EM INFORMÁTICA
Interface Tecnológica · v. 23, n. 1, 2026 · p. 10–17
ISSN on-line 2447-0864 · ISSN impresso 1807-3980
https://doi.org/10.31510/infa.v23i1.2399

OS IMPACTOS DO RECONHECIMENTO FACIAL NO CONTROLE DE ACESSO DE PESSOAS NAS INSTITUIÇÕES PÚBLICAS DE ENSINO

The impacts of facial recognition on access control of people in public educational institutions

Ariadne Saraiva dos Santos[1], **Nubia Abreu de Oliveira**[2], **Jonatas Cerqueira Dias**[3]

AUTORIA

[1] **Ariadne Saraiva dos Santos**
Fatec Praia Grande – SP – Brasil
ariadne.santos2@fatec.sp.gov.br
ORCID: https://orcid.org/0009-0005-2167-472X

[2] **Nubia Abreu de Oliveira**
Fatec Praia Grande – SP – Brasil
nubia.oliveira4@fatec.sp.gov.br
ORCID: https://orcid.org/0009-0000-3065-8776

[3] **Jonatas Cerqueira Dias**
Fatec Praia Grande – SP – Brasil
jonatas.dias2@fatec.sp.gov.br
ORCID: 0000-0003-2515-8018

HISTÓRICO

Recebido	18/03/2026
Aceito	04/06/2026
Publicado	30/06/2026

COMO CITAR

SANTOS, A. S.; OLIVEIRA, N. A.; DIAS, J. C. Os impactos do reconhecimento facial no controle de acesso de pessoas nas instituições públicas de ensino. **Interface Tecnológica**, Taquaritinga, v. 23, n. 1, p. 10-17, 2026. DOI: 10.31510/infa.v23i1.2399.

LICENÇA

Artigo de acesso aberto distribuído sob a licença Creative Commons Atribuição 4.0 Internacional.

cc BY 4.0

RESUMO

Este artigo analisa os impactos do uso da tecnologia de reconhecimento facial no controle de acesso em instituições públicas de ensino considerando quesitos como segurança e privacidade, implicações éticas e legais, precisão dos algoritmos e custo de implementação. A crescente adoção dessa tecnologia por escolas públicas brasileiras pretende enfrentar desafios na segurança, no entanto, seu uso levanta preocupações quanto à privacidade, discriminação algorítmica, custos de implementação e ausência de regulamentações específicas. A fundamentação trata da segurança pública e a importância no controle de acesso de pessoas, do que é o reconhecimento facial, os principais algoritmos utilizados, seus níveis de precisão, e os riscos associados ao armazenamento de dados biométricos sensíveis. A metodologia empregada foi a revisão bibliográfica, com análise de estudos científicos, relatórios técnicos e experiências práticas documentadas. Como resultado, observou-se que, embora o reconhecimento facial ofereça benefícios operacionais, sua adoção sem o devido planejamento, transparência e respeito aos direitos fundamentais pode comprometer a segurança jurídica e ética do ambiente escolar. Conclui-se que o uso dessa tecnologia deve ser acompanhado de regulamentação clara, estudos de impacto e participação da comunidade escolar nas decisões de sua implementação.

Palavras-chave: Instituições públicas de ensino. Reconhecimento facial. Ética tecnológica. Gestão escolar. Proteção de dados.

ABSTRACT

This article analyzes the impacts of using facial recognition technology in access control in public educational institutions, considering aspects such as security and privacy, ethical and legal implications, algorithm accuracy and implementation costs. The growing adoption of this technology by Brazilian public schools aims to address security challenges; however, its use raises concerns about privacy, algorithmic discrimination, implementation costs, and the lack of specific regulations. The rationale addresses public safety and its importance in controlling people's access, what facial recognition is, the main algorithms used, their levels of accuracy, and the risks associated with storing sensitive biometric data. The methodology used was a literature review, with analysis of scientific studies, technical reports, and documented practical experiences. As a result, it was observed that, although facial recognition offers operational benefits, its adoption without proper planning, transparency, and respect for fundamental rights can compromise the legal and ethical security of the school environment. It is concluded that

the use of this technology must be accompanied by clear regulations, impact studies, and participation of the school community in decisions regarding its implementation.

Keywords: Public educational institutions. Facial recognition. Technological ethics. School management. Data protection.

1 INTRODUÇÃO

A segurança física em instituições públicas de ensino tem sido uma preocupação crescente diante de desafios como violência, evasão escolar e acesso não autorizado a ambientes escolares. Neste contexto, o uso de tecnologias de reconhecimento facial tem se destacado como uma solução tecnológica promissora para o controle de acesso e monitoramento de alunos e visitantes. Diversos municípios brasileiros vêm adotando sistemas baseados em biometria facial com o intuito de otimizar a gestão escolar, garantir a presença de estudantes em sala de aula e, principalmente, aumentar a segurança nas dependências das escolas (TAVARES *et al*., 2023).

Embora a proposta seja vista por alguns gestores como um avanço na modernização do ambiente educacional, essa tecnologia levanta debates sobre privacidade, consentimento, discriminação algorítmica e eficácia prática. Especialistas alertam que, apesar da popularização do reconhecimento facial, sua aplicação em espaços educacionais ainda carece de estudos sobre impactos nos direitos fundamentais de crianças e adolescentes, bem como de regulamentações específicas que orientem sua implementação (UNIVERSIDADE TIRADENTES, 2024; JAZAR *et al*., 2023).

O caso do Paraná é emblemático: entre 2022 e 2023, a tecnologia foi implementada em 1.667 escolas públicas por meio do programa Educação para o Futuro, com o objetivo de combater a evasão escolar e garantir maior controle de frequência (JAZAR *et al*., 2023). No entanto, essa medida também gerou críticas sobre a redução da autonomia docente e preocupações quanto ao uso e armazenamento dos dados biométricos dos alunos, especialmente à luz da Lei Geral de Proteção de Dados (LGPD).

De acordo com Tavares *et al.* (2023), a adoção de tecnologias como o reconhecimento facial nas escolas públicas brasileiras muitas vezes desvia o foco das verdadeiras necessidades do sistema educacional, como investimentos em infraestrutura, valorização dos profissionais da educação e melhoria das condições de aprendizagem. Diante desse cenário, este artigo tem como objetivo geral analisar, por meio de revisão bibliográfica, os impactos do reconhecimento facial no controle de acesso em instituições públicas de ensino, avaliando como a tecnologia pode contribuir para a segurança sem comprometer os direitos fundamentais da comunidade escolar. Como objetivos específicos, o estudo propõe-se a: investigar as implicações éticas e legais frente à LGPD; discutir a precisão e os riscos de discriminação algorítmica; e refletir sobre a viabilidade econômica dessas ferramentas. A pesquisa justifica-se pela relevância e atualidade do tema, dado o impacto direto da gestão de dados biométricos na privacidade de alunos e docentes.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 Segurança pública e a importância do controle de acesso de pessoas

Segundo Vedova (2023), a segurança pública deve ser compreendida como um sistema amplo e integrado que vai além das ações repressivas do Estado, envolvendo também políticas de prevenção, inclusão social e garantia dos direitos fundamentais. Ela representa um instrumento base para a convivência democrática, sendo responsabilidade não apenas do poder público, mas de toda a sociedade.

De acordo com Rodrigues (2023), a proteção de dados pessoais vai além do ambiente digital, pois é no mundo físico que se encontram os ativos que sustentam a infraestrutura tecnológica, como servidores e equipamentos de rede. Assim, o controle de acesso físico é o que garante a conformidade com a Lei Geral de Proteção de Dados (LGPD), já que não é possível implantar medidas eficazes de segurança da informação sem considerar os meios físicos que armazenam e processam os dados.

2.2 Reconhecimento facial e algoritmos de identificação

Conforme Santos *et al.* (2023), o reconhecimento facial é uma tecnologia biométrica que identifica indivíduos por meio da análise matemática de características únicas do rosto. Ainda segundo o autor, o processo envolve três etapas: (1) detecção de pontos faciais-chave como a distância entre olhos, formato da mandíbula, profundidade das órbitas oculares e outros 84 pontos faciais, convertendo-os em um código numérico único, (2) criação de uma "assinatura facial" (fórmula matemática baseada nas características) e (3) comparação com um banco de dados pré-existente para verificação ou identificação.

O estudo de Braga (2023) detalha a implementação prática: sistemas utilizam algoritmos para detecção facial e Análise Discriminante Linear (LDA) para extração de características, alcançando até 72,37% de precisão em ambientes movimentados. Segundo ela, a tecnologia evoluiu de métodos rudimentares (como PCA – *Principal Component Analysis*) para redes neurais convolucionais (CNNs), que melhoram a adaptação a variações de iluminação e ângulo.

2.3 Precisão dos algoritmos

Pessoa (2019) define Eigenfaces como o conjunto de autovetores de uma matriz contendo imagens de rostos. Ainda segundo ele, a técnica foi desenvolvida por Sirovich e Kirby ao tratar dos padrões encontrados em imagens de rostos utilizando o método de Análise de Componentes Principais (sigla PCA em inglês).

Segundo Silva *et al*. (2021), o algoritmo Fisherfaces utiliza uma matriz de transformação voltada para a diferenciação entre classes, reduzindo a influência da iluminação, o que o torna distinto do método Eigenfaces.

De acordo com Silva (2023), o algoritmo LBPH combina as técnicas de Local Binary Pattern (LBP) e Histogram Oriented Gradients (HOG), sendo reconhecido por sua alta precisão, inclusive em diferentes ângulos faciais, como de frente e de lado.

2.4 Custos

Tavares *et al.* (2023) indicam que a implementação de tecnologias de reconhecimento facial nas escolas ocorre principalmente por meio de licitações e que envolve custos significativos, que variam amplamente entre os municípios. Ainda segundo eles, o contrato feito no município de Goiânia apresentou o valor R$ 9.379.305,00, enquanto o contrato feito no município de Xaxim apresentou o valor de R$ 55.680,00. Os autores destacam que alguns locais enfrentam desafios orçamentários, o que levanta questões sobre a viabilidade financeira de tais projetos em um contexto de escassez de recursos para a educação. Também aponta que, embora a tecnologia de reconhecimento facial seja apresentada como uma solução para otimizar a gestão escolar e reduzir custos operacionais, a realidade é que os investimentos iniciais e os custos de manutenção podem ser

elevados, o que pode desviar recursos de outras áreas essenciais da educação, como infraestrutura e formação de professores.

2.5 Regulamentação e segurança

Segundo uma matéria adaptada de dados do Serpro a Lei Geral de Proteção de Dados (LGPD) trata da proteção dos direitos fundamentais de liberdade e privacidade, criando um ambiente de segurança jurídica para o tratamento de dados pessoais no Brasil. Segundo a LGPD, todos os dados tratados, sejam em meio físico ou digital, estão sujeitos à regulação, assegurando que a proteção se aplique a qualquer informação que possa identificar uma pessoa (MPF, 2025).

A ISO 27001 é uma norma internacional para a gestão da segurança da informação na proteção da confidencialidade, integridade e disponibilidade dos dados, independentemente do tipo de organização. Embora a ISO 27001 e a LGPD tratem de aspectos relacionados à segurança da informação, a certificação na norma não garante que uma empresa esteja em conformidade com as exigências da LGPD, que regula especificamente a coleta e o tratamento de dados pessoais (BASQUES, 2025). Godoy e Morastico (2019) propõem o reconhecimento facial como uma solução para melhorar a segurança física em ambientes corporativos, atendendo regulamentações como ISO 27001:2013 e LGPD.

O artigo de Silva, Franqueira e Hartmann (2021) destaca a ausência de normas específicas que regulem o uso dessa tecnologia. Segundo os autores, a legislação em muitos países da América Latina ainda não é suficiente para abordar as particularidades do reconhecimento facial, o que gera preocupações quanto à proteção de dados pessoais e à transparência no uso dessas ferramentas. A falta de uma regulamentação eficaz tem sido apontada como um fator que contribui para a violação de direitos fundamentais, como a privacidade e a liberdade de expressão. Os autores sugerem a implementação de diretrizes claras, que incluam mecanismos de auditoria independente, transparência e responsabilização.

2.6 Riscos à privacidade

Segundo o professor Calasans, o armazenamento inadequado de dados faciais pode expor os cidadãos a sérios riscos, como roubo de identidade e fraudes, uma vez que os dados biométricos são permanentes e não podem ser alterados como senhas convencionais. Além disso, observa que os algoritmos de reconhecimento facial podem apresentar falhas significativas na identificação de indivíduos de diferentes etnias, gêneros ou idades, o que levanta preocupações sobre discriminação (UNIVERSIDADE TIRADENTES, 2024).

Tavares *et al.* (2023) destacam que a adoção de tecnologias de reconhecimento facial nas escolas levanta sérias preocupações em relação à privacidade dos estudantes, uma vez que esses sistemas coletam e armazenam dados biométricos sensíveis. Destacam ainda que a falta de estudos de impacto sobre os direitos humanos antes da implementação dessas tecnologias é um ponto crítico, pois pode resultar em violações da privacidade e da dignidade dos alunos.

3 PROCEDIMENTOS METODOLÓGICOS

Conforme Canuto e Oliveira (2020), os estudos de revisão bibliográfica são caracterizados pela análise de publicações científicas já consolidadas, como livros, artigos, teses e dissertações, sem recorrer diretamente à observação de fenômenos empíricos. Esse tipo de pesquisa utiliza fontes secundárias, ou seja, interpretações e discussões elaboradas por outros autores sobre determi-

nado tema. Sendo assim, a presente pesquisa se caracteriza como uma revisão bibliográfica, uma vez que permitiu a elaboração de uma tabela comparativa com itens que favorecem ou desfavorecem a aplicação do reconhecimento facial.

Os critérios analisados foram extraídos de estudos científicos e técnicos, e organizados de forma a permitir uma análise qualitativa das facilidades e limitações do uso do reconhecimento facial, pois, segundo Pereira (2013), a seção de resultados de um artigo científico tem como principal função apresentar de forma clara e objetiva os dados obtidos ao longo da pesquisa, sintetizando apenas as informações mais relevantes, sem incluir interpretações ou discussões, que devem ser reservadas para seções específicas do trabalho.

4 RESULTADOS E DISCUSSÃO

Esta seção apresenta os resultados obtidos a partir da pesquisa bibliográfica e discute os principais impactos dessa tecnologia no ambiente estudantil. A análise permitiu identificar aspectos importantes da adoção do reconhecimento facial no ambiente escolar, especialmente quanto à segurança, precisão dos algoritmos, custos, regulamentação e privacidade. Foi possível perceber, conforme Tavares *et al.* (2023), que a tecnologia contribui para maior agilidade no controle de entrada e saída de pessoas, reduzindo a necessidade de intervenção humana e favorecendo uma gestão mais eficiente dos fluxos nos ambientes escolares. Essa automação amplia o monitoramento em tempo real e fortalece a rastreabilidade dos acessos para a proteção de alunos, professores e funcionários.

Sobre o desempenho dos algoritmos de reconhecimento facial, estudos como os de Braga (2023), Silva *et al.* (2021) e Silva (2023) demonstram que técnicas como Eigenfaces, Fisherfaces e LBPH podem alcançar bons níveis de precisão quando utilizadas em ambientes adequados e com bancos de dados estruturados. Isso é um fator positivo no uso dessa tecnologia como auxílio no controle de acesso de pessoas. No entanto, como destaca a Universidade Tiradentes (2024), isso não impede a ocorrência de falhas decorrentes de fatores como iluminação, ângulos de captura e possíveis discriminações algorítmicas relacionadas a etnia, idade ou gênero, lembrando a necessidade de abordagens criteriosas na implementação.

Outro fator importante observado é acerca dos desafios legais e éticos. Pesquisas de Silva, Franqueira e Hartmann (2021) apontam que a ausência de regulamentação específica para o uso de reconhecimento facial na América Latina eleva o risco de uso inadequado dos dados e compromete direitos fundamentais. Por outro lado, autores como Basques (2025) e Godoy e Morastico (2019) afirmam que, quando alinhada à Lei Geral de Proteção de Dados (LGPD) e a práticas de segurança da informação, essa tecnologia pode apresentar resultados muito positivos. MPF (2025) corrobora o descrito anteriormente, chamando a atenção para que haja clareza nas finalidades de uso, transparência no tratamento dos dados e mecanismos de responsabilização.

Quanto aos custos, Tavares *et al.* (2023) evidenciam que os investimentos iniciais podem ser elevados, especialmente pela necessidade de infraestrutura, equipamentos e capacitação profissional. Apesar disso, os autores também apontam que a médio e longo prazo os benefícios relacionados à segurança, automação e eficiência operacional tendem a superar os gastos iniciais, tornando a adoção viável em muitos contextos educacionais.

A questão da privacidade se mostrou um ponto de atenção. Conforme alerta a Universidade Tiradentes (2024), dados biométricos são permanentes e, se vazados, não podem ser substituídos como senhas convencionais.

Por meio do que foi obtido nos estudos de Tavares *et al.* (2023), Silva *et al.* (2021), Silva (2023), Braga (2023), Basques (2025), Godoy e Morastico (2019), Universidade Tiradentes (2024) e MPF (2025), foi possível construir o Quadro 1, que sintetiza os principais critérios analisados e compara os aspectos que favorecem e desfavorecem o uso do reconhecimento facial no controle de acesso escolar. Nesse comparativo, é possível observar como segurança, precisão dos algoritmos e eficiência operacional surgem como pontos fortes, enquanto privacidade, custos e regulamentação se destacam como desafios que exigem atenção constante.

Quadro 1 – Critérios acerca do reconhecimento facial

Critério	Favorece	Desfavorece
Segurança e controle de acesso	Aumenta a agilidade na entrada e saída de pessoas; Reduz intervenção humana na verificação; Auxilia na inibição de entradas não autorizadas; Melhora o controle de presença e monitoramento em escolas.	Vulnerabilidades decorrentes de má implementação podem gerar falhas; Risco de erros de identificação (falhas com etnias, idades e gêneros: discriminação algorítmica); Possível uso inadequado do armazenamento de dados.
Precisão dos algoritmos	Algoritmos Eigenface, Fisherface e LBPH alcançam bons níveis de precisão quando utilizados corretamente; CNNs aumentam precisão mesmo com variação de iluminação.	Algoritmos são sensíveis a variações de iluminação, ângulo e oclusões; Podem ter desempenho inferior para alguns grupos (gênero, etnia, idade).
Custo de implementação	Pode otimizar a gestão escolar e reduzir custos operacionais a longo prazo.	Alto investimento inicial; Custos de manutenção e infraestrutura podem ser elevados.
Regulamentação	Possibilidade de estar em conformidade com normas como LGPD e ISO 27001 quando bem implementado.	Ausência de normas específicas para reconhecimento facial na América Latina; Falta de regulamentação clara aumenta riscos de violação de direitos fundamentais.
Privacidade	Possibilidade de aplicar consentimento, transparência e políticas de segurança, quando bem gerido.	Dados biométricos são sensíveis e permanentes; se vazarem, não podem ser alterados; Risco de vigilância excessiva e monitoramento indevido; Falta de estudos de impacto sobre direitos humanos.

Fonte: Elaborado pelos autores (2025).

5 CONCLUSÃO

A implementação do reconhecimento facial como ferramenta de controle de acesso em instituições públicas de ensino representa um avanço significativo no que se refere à modernização da segurança e à eficiência na gestão dos espaços escolares. Ao longo deste estudo, foi possível identificar que essa tecnologia oferece benefícios expressivos, como a automação do processo de entrada e saída de pessoas, a redução da intervenção humana, o aumento da precisão no controle de acessos e a inibição de entradas não autorizadas. Contudo, a adoção dessa tecnologia envolve não apenas questões técnicas e operacionais, mas também importantes reflexões sociais e éticas.

A presença de sistemas de vigilância biométrica em ambientes educacionais levanta preocupações legítimas relacionadas à privacidade, ao consentimento dos usuários e ao risco de uso indevido dos dados pessoais. Nesse sentido, é fundamental que a implantação de sistemas de reconhecimento facial esteja em conformidade com a Lei Geral de Proteção de Dados (LGPD), respeitando os princípios de transparência, segurança, necessidade e finalidade no tratamento das informações sensíveis dos indivíduos. Ainda deve-se considerar o impacto social causado pela sensação de constante vigilância. Em contextos educacionais, onde a liberdade, a inclusão e a confiança são necessários para o desenvolvimento humano, é preciso equilibrar o uso da tecnologia

com o bem-estar dos alunos, professores e demais integrantes da comunidade acadêmica. A implantação deve ser acompanhada por ações de conscientização, consulta pública e participação dos usuários no processo decisório.

Conclui-se, portanto, que o reconhecimento facial possui potencial para transformar positivamente a forma como o acesso é gerenciado em instituições públicas de ensino, promovendo maior segurança, controle e eficiência. Mas, sua aplicação deve ser conduzida com responsabilidade, ética e respeito aos direitos individuais. O uso consciente dessa tecnologia, aliado a políticas claras de proteção de dados e à valorização do diálogo com a comunidade, pode contribuir significativamente para uma gestão educacional mais moderna, segura e socialmente justa.

REFERÊNCIAS

BASQUES. **Entenda a relação entre ISO 27001 e LGPD**. [*S. l.*: *s. n.*], 2025. Disponível em: https://blwinner.com.br/blog/entenda-a-relacao-entre-iso-27001-e-lgpd/. Acesso em: 11 fev. 2025.

BRAGA, L. F. Z. **Sistemas de reconhecimento facial**. 2023. Universidade de São Paulo, 2023. Disponível em: https://bdta.abcd.usp.br/directbitstream/46b694a0-715b-462d-a8b7-546ea4ef259d/Braga_Luiz_Filipe_Zenicola.pdf. Acesso em: 6 fev. 2025.

CANUTO, Lívia Teixeira; OLIVEIRA, Adélia Augusta Souto de. Métodos de revisão bibliográfica nos estudos científicos. **Psicologia em Revista**, v. 26, n. 1, p. 82-100, 2020. DOI: https://doi.org/10.5752/P.1678-9563.2020v26n1p82-100.

GODOY, Samuel Pereira de; MORASTICO, Andrey Cesar. **Segurança física com reconhecimento facial**. 2019. Trabalho de Conclusão de Curso (Graduação em Engenharia de Computação) – Centro Universitário Uninter, Curitiba, 2019.

JAZAR, M. M. *et al.* **Reconhecimento facial nas escolas públicas do Paraná**: relatório 2023. [*S. l.*: *s. n.*], 2023. Disponível em: https://www.observatoriodasmetropoles.net.br/wp-content/uploads/2023/11/Relatorio_Reconhecimento-Facial_2023.pdf. Acesso em: 23 mar. 2025.

MPF. **O que é a LGPD?** [*S. l.*: *s. n.*, *s. d.*]. Disponível em: https://www.mpf.mp.br/servicos/lgpd/o-que-e. Acesso em: 11 fev. 2025.

PEREIRA, Mauricio Gomes. A seção de resultados de um artigo científico. **Epidemiologia e Serviços de Saúde**, v. 22, n. 2, p. 353-354, jun. 2013. Disponível em: https://bvsms.saude.gov.br/bvs/periodicos/epidemiologia_servicos_saude_volume22_n2.pdf. Acesso em: 28 mar. 2025.

PESSOA, Willian. **Reconhecimento de padrões — Eigenfaces**. Medium, 12 jun. 2019. Disponível em: https://medium.com/@williangpessoa/reconhecimento-de-padr%C3%B5es-eigenfaces-e4cef8f04919. Acesso em: 5 mar. 2025.

RODRIGUES, Fabrizio. **A importância do controle de acesso físico**. JusBrasil, 2023. Disponível em: https://www.jusbrasil.com.br/artigos/a-importancia-do-controle-de-acesso-fisico/886526945. Acesso em: 28 mar. 2025.

SANTOS, Lucas Gabriel de Matos *et al.* Reconhecimento facial: tecnologia, racismo e construção de mundos possíveis. **Psicologia & Sociedade**, [*s. l.*], v. 35, e277141, 2023. DOI: https://doi.org/10.1590/1807-0310/2023v35e277141. Acesso em: 6 jan. 2025.

SILVA, E. V. C. **Avaliação de algoritmos de reconhecimento facial para autenticação de usuários**. 2023. Trabalho de Conclusão de Curso (Bacharelado em Ciência da Computação) – Universidade Federal de Uberlândia, Uberlândia, 2023. Disponível em: https://repositorio.ufu.br/bitstream/123456789/41074/3/Avalia%C3%A7%C3%A3oAlgoritmosReconhecimento.pdf. Acesso em: 28 mar. 2025.

SILVA, J. L.; OLIVEIRA, I.; TOPOLNIAK, Z. H.; ALVAREZ, A. B. Estudo e análise de técnicas de visão computacional para reconhecimento de expressões faciais no monitoramento individual visando a prevenção de colapsos autistas. **Revista Conexão na Amazônia**, v. 3, n. 2, p. 147-167, 2021.

SILVA, Lorena Abbas da; 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: https://doi.org/10.11606/issn.2319-0558.v8i1p171-204. Disponível em: https://www.revistas.usp.br/rdda/article/view/173903. Acesso em: 10 nov. 2024.

TAVARES, C.; SIMÃO, B.; MARTINS, F.; SANTOS, B.; ARAÚJO, A. **Tecnologias de vigilância e educação**: um mapeamento das políticas de reconhecimento facial em escolas públicas brasileiras. São Paulo: InternetLab, 2023. Disponível em: https://internetlab.org.br/wp-content/uploads/2023/06/Educacao-na-mira-PT_06.pdf. Acesso em: 28 mar. 2025.

UNIVERSIDADE TIRADENTES. **Reconhecimento facial traz desafios para a privacidade e proteção de dados**. [*S. l.*], 2024. Disponível em: https://portal.unit.br/blog/noticias/reconhecimento-facial-traz-desafios-para-a-privacidade-e-protecao-de-dados/. Acesso em: 12 dez. 2024.

VEDOVA, Daiane. **O que é segurança pública**. JusBrasil, 2023. Disponível em: https://www.jusbrasil.com.br/artigos/o-que-e-seguranca-publica/586735267. Acesso em: 28 mar. 2025.

Os conceitos e as opiniões expressos neste artigo são de responsabilidade exclusiva de seus autores.