

VISÃO COMPUTACIONAL PARA RECONHECIMENTO FACIAL: AVANÇOS E RISCOS <https://doi.org/10.63330/aurumpub.021-011>**Rodrigo Thomé de Moura**

Pós-graduação em Dança Terapia

Prisma

E-mail: rodrigofsw@gmail.com

RESUMO

O trabalho apresentou uma análise abrangente sobre a visão computacional aplicada ao reconhecimento facial, destacando seus avanços técnicos e os riscos associados ao uso dessa tecnologia em contextos contemporâneos. O estudo teve como objetivo explicar os fundamentos da visão computacional, descrever o funcionamento técnico dos algoritmos de reconhecimento facial, identificar os principais avanços que ampliaram a precisão e a disseminação desses sistemas e discutir os desafios éticos e sociais decorrentes de sua utilização crescente. A pesquisa foi desenvolvida por meio de revisão bibliográfica, baseada em obras e estudos relevantes da área de inteligência artificial, visão computacional, aprendizado profundo e ética tecnológica. A metodologia permitiu reunir, interpretar e comparar diferentes perspectivas teóricas e técnicas sobre o tema, possibilitando uma compreensão sólida e crítica do fenômeno analisado. Os resultados mostraram que o reconhecimento facial evoluiu de maneira acelerada devido ao desenvolvimento das redes neurais profundas, ao aumento da capacidade computacional e ao acesso a grandes bases de dados de imagens. A precisão desses modelos aumentou significativamente, levando à implementação da tecnologia em dispositivos móveis, sistemas de controle de acesso, plataformas digitais e aplicações de segurança. No entanto, o trabalho identificou riscos importantes, como violações de privacidade, uso indevido de dados biométricos, vigilância massiva, vieses algorítmicos que afetam com maior intensidade grupos minoritários e vulnerabilidades associadas a técnicas de falsificação digital. A análise concluiu que, embora o reconhecimento facial represente um avanço significativo dentro da inteligência artificial, seu uso exige regulamentação, transparência e práticas responsáveis para evitar danos sociais e assegurar a proteção dos direitos individuais. O estudo evidenciou a necessidade de equilíbrio entre inovação tecnológica e ética, apontando caminhos que favorecem a aplicação segura e consciente dessa ferramenta.

Palavras-chave: Reconhecimento facial; Visão computacional; Inteligência Artificial; Privacidade; Ética.



1 INTRODUÇÃO

A rápida evolução da Inteligência Artificial tem transformado profundamente a forma como indivíduos, instituições e sistemas tecnológicos interagem com o mundo digital. Entre essas inovações, a visão computacional destaca-se como uma das áreas mais dinâmicas, por permitir que máquinas interpretem e processem informações visuais de maneira cada vez mais semelhante ao ser humano. Dentro desse campo, o reconhecimento facial tornou-se uma das aplicações mais difundidas, presente em smartphones, plataformas digitais, sistemas de segurança e mecanismos de autenticação automática. A literatura especializada aponta que essa tecnologia, impulsionada principalmente pelo avanço das redes neurais convolucionais e do deep learning, alcançou níveis de precisão antes considerados inalcançáveis (Szeliski, 2022; Goodfellow; Bengio; Courville, 2016). Contudo, esse desenvolvimento acelerado também levanta preocupações éticas, sociais e técnicas que exigem análise cuidadosa.

Desse modo, o presente trabalho tem como tema a visão computacional aplicada ao reconhecimento facial, com foco nos seus avanços recentes e nos riscos associados ao seu uso. Este estudo parte da compreensão de que a tecnologia, apesar de extremamente útil para autenticação biométrica, controle de acesso, segurança pública e personalização de recursos digitais, traz desafios significativos relacionados à privacidade, ao tratamento de dados pessoais e à possibilidade de uso indevido. A literatura consultada reforça tais preocupações, destacando, por exemplo, os elevados índices de erro em mulheres, negros e minorias (Buolamwini; Gebru, 2018), os riscos de vigilância massiva (Lyon, 2018) e a crescente sofisticação de falsificações digitais e *deepfakes* (Tolosana et al., 2020).

O objetivo geral deste trabalho é analisar criticamente os avanços técnicos do reconhecimento facial e discutir os riscos e desafios decorrentes de sua expansão. Como objetivos específicos, busca-se: explicar os conceitos fundamentais da visão computacional e do processamento de imagens; descrever o funcionamento técnico do reconhecimento facial e seus principais algoritmos; apresentar os avanços que tornaram essa tecnologia mais precisa e acessível; e, por fim, analisar seus riscos éticos, sociais e de segurança à luz da literatura atual. Parte-se da hipótese de que, embora o reconhecimento facial represente um marco no desenvolvimento da inteligência artificial, seu uso indiscriminado e sem regulação adequada pode gerar impactos negativos significativos, especialmente no que se refere à privacidade e à equidade social.

A justificativa deste estudo encontra-se na relevância contemporânea do tema. Em um contexto no qual câmeras, sensores e sistemas algoritmos se tornam onipresentes, compreender o funcionamento e os impactos dessa tecnologia é fundamental para que cidadãos, profissionais e instituições adotem práticas responsáveis e alinhadas à legislação vigente. Além disso, diante da crescente inserção da biometria facial em espaços públicos e privados, torna-se urgente debater limites, riscos e possibilidades, contribuindo para um uso mais seguro, justo e consciente dessas ferramentas.



Por fim, este trabalho foi desenvolvido por meio de pesquisa bibliográfica, baseada em autores clássicos e contemporâneos da área de visão computacional, aprendizado profundo e ética em inteligência artificial. Ao longo do estudo, são apresentados conceitos fundamentais, o funcionamento técnico dos sistemas, seus avanços recentes e as problemáticas éticas e sociais decorrentes de seu uso, permitindo uma visão ampla, crítica e fundamentada do tema.

2 METODOLOGIA

O trabalho foi desenvolvido por meio de uma pesquisa bibliográfica, com abordagem qualitativa, fundamentada na seleção, análise e interpretação de obras, artigos científicos e documentos técnicos relacionados à visão computacional, reconhecimento facial, aprendizado profundo e ética em inteligência artificial. A escolha desse método permitiu compreender de forma ampla e crítica a evolução tecnológica, o funcionamento dos algoritmos e os impactos sociais associados ao uso crescente dessa tecnologia. A pesquisa bibliográfica foi conduzida com base em autores clássicos e contemporâneos da área, possibilitando a construção de um referencial teórico sólido e coerente. O processo metodológico incluiu a identificação de publicações relevantes em bases acadêmicas, revistas científicas e livros especializados, priorizando materiais que discutiram de maneira aprofundada os aspectos técnicos, os avanços recentes e os riscos envolvidos no reconhecimento facial. Após essa seleção, os conteúdos foram analisados e organizados em categorias temáticas, permitindo a estruturação dos tópicos abordados no desenvolvimento do trabalho. Esse procedimento possibilitou comparar perspectivas, sintetizar informações e discutir criticamente os desafios éticos e tecnológicos relacionados ao tema. Dessa forma, a metodologia adotada garantiu consistência teórica e contribuiu para uma análise abrangente, produzindo um estudo alinhado às exigências acadêmicas e ao propósito de compreender tanto os avanços quanto as preocupações que permeiam o uso da visão computacional aplicada ao reconhecimento facial.

3 DESENVOLVIMENTO

3.1 VISÃO COMPUTACIONAL: CONCEITOS BÁSICOS

A visão computacional constitui um dos campos mais dinâmicos da Inteligência Artificial, pois busca permitir que máquinas interpretem, analisem e compreendam informações visuais de maneira semelhante ao ser humano. De forma ampla, pode ser definida como o conjunto de técnicas, algoritmos e modelos computacionais capazes de extrair, processar e reconhecer padrões em imagens e vídeos, atribuindo significado a esses dados para a realização de tarefas específicas. Segundo Szeliski (2022), a visão computacional se fundamenta na capacidade de transformar dados visuais brutos em representações estruturadas, possibilitando que sistemas automatizados realizem desde atividades simples, como detectar bordas em uma imagem, até operações complexas, como identificar rostos, objetos ou ações em movimento.

O processamento de imagens, por sua vez, constitui uma etapa essencial dentro da visão computacional. Ele engloba procedimentos matemáticos e computacionais que visam melhorar, transformar ou analisar imagens, permitindo que o sistema extraia informações relevantes para o reconhecimento visual. Entre as técnicas mais comuns estão a filtragem, segmentação, detecção de contornos e transformação de cores — métodos fundamentais para reduzir ruído, realçar detalhes e separar os elementos significativos da imagem para posterior interpretação. De acordo com Gonzalez e Woods (2018), o processamento de imagens é a base sobre a qual algoritmos mais avançados são construídos, funcionando como um elo entre a captura da informação visual e a compreensão automatizada realizada pela IA.

Nos últimos anos, o avanço mais significativo na área ocorreu com o desenvolvimento das redes neurais convolucionais (CNNs) e do deep learning. As CNNs são modelos profundamente inspirados na organização do córtex visual humano e se destacam por sua capacidade de identificar padrões complexos diretamente a partir dos dados, sem a necessidade de extrair manualmente características visuais. LeCun, Bengio e Hinton (2015) ressaltam que esse tipo de rede revolucionou o campo da visão computacional por conseguir processar imagens de forma hierárquica: nas primeiras camadas, identificam-se traços simples como bordas e texturas; nas camadas mais profundas, surgem representações abstratas que descrevem objetos completos, rostos ou cenas.

O deep learning ampliou ainda mais esse potencial, permitindo o treinamento de redes com dezenas ou centenas de camadas para realizar tarefas como reconhecimento facial, classificação de imagens, detecção de anomalias, segmentação semântica e muitas outras aplicações. Essas arquiteturas profundas aprendem de modo autônomo a partir de grandes volumes de dados, o que torna seu desempenho altamente superior ao de métodos tradicionais em diversas tarefas visuais. Como afirmam Goodfellow, Bengio e Courville (2016), o deep learning possibilitou que a visão computacional atingisse níveis de precisão próximos — e em alguns casos superiores — aos do ser humano, especialmente em ambientes controlados.

Assim, compreender os conceitos básicos de visão computacional, processamento de imagens e redes neurais convolucionais é fundamental para estudar as aplicações contemporâneas do reconhecimento visual por máquinas. Esses fundamentos teóricos sustentam os avanços atuais e oferecem uma base sólida para a análise crítica dos usos, limitações e implicações éticas das tecnologias baseadas em visão artificial.

3.2 RECONHECIMENTO FACIAL: FUNCIONAMENTO TÉCNICO

O reconhecimento facial, dentro do campo da visão computacional, constitui um processo técnico complexo que envolve múltiplas etapas destinadas a identificar ou verificar a identidade de indivíduos a partir de imagens ou vídeos. Seu funcionamento moderno está profundamente ligado ao uso de redes neurais profundas, que possibilitam a análise precisa de padrões visuais. Para que essa tecnologia opere, o sistema precisa inicialmente detectar e localizar um rosto na imagem; em seguida, analisar suas



características estruturais; e, por fim, compará-las com um banco de dados previamente registrado. Segundo Zhao et al. (2003), o reconhecimento facial combina técnicas de detecção, extração de características e classificação, formando um pipeline que transforma uma face em informações numéricas capazes de representar a identidade de uma pessoa.

A primeira etapa, a detecção facial, consiste em encontrar a região exata em que o rosto está presente. Algoritmos clássicos, como o Haar Cascade de Viola e Jones, foram amplamente utilizados por sua rapidez e eficiência. Entretanto, abordagens modernas, como MTCNN (Multi-Task Cascaded Convolutional Networks), SSD e YOLO, oferecem maior precisão, sendo capazes de identificar rostos sob variações de iluminação, ângulo e expressão. Após detectar o rosto, inicia-se a análise de padrões faciais, que envolve a identificação de elementos estruturais como posição dos olhos, formato do nariz, contorno do rosto e distância entre pontos específicos. Essa análise permite captar a geometria facial, que Bojanowski e Joulin (2017) destacam como essencial para representar a identidade de forma consistente, mesmo diante de pequenas variações de pose.

A etapa seguinte, e talvez a mais crucial, é a extração de características faciais. Nos modelos modernos, essa extração ocorre por meio das redes neurais convolucionais, que transformam o rosto em um vetor numérico de alta dimensão, conhecido como *embedding facial*. Esse embedding funciona como uma espécie de "assinatura digital" da face, representando padrões únicos da pessoa de forma compacta e comparável. O sistema então utiliza métricas de similaridade — como distância euclidiana ou cosseno — para comparar o vetor do rosto analisado com vetores armazenados no banco de dados. Quanto menor a distância entre dois embeddings, maior a probabilidade de se referirem à mesma pessoa. De acordo com Schroff, Kalenichenko e Philbin (2015), essa abordagem permitiu que o reconhecimento facial alcançasse níveis de precisão antes considerados impossíveis. Diversos algoritmos e bases de dados contribuíram significativamente para o desenvolvimento desses sistemas. O *Labeled Faces in the Wild* (LFW), por exemplo, tornou-se um dos primeiros benchmarks de grande impacto, permitindo avaliar a precisão dos modelos em condições reais e não controladas. O VGGFace, desenvolvido pelo Visual Geometry Group, ampliou ainda mais esse campo ao disponibilizar uma base robusta e um modelo pré-treinado de alta performance. Já o FaceNet, proposto por Schroff et al. (2015), revolucionou o reconhecimento facial ao introduzir o conceito de *triplet loss*, que otimiza diretamente as distâncias entre embeddings, aumentando a precisão do modelo em tarefas de verificação e identificação. Esses avanços permitiram que a tecnologia fosse incorporada em smartphones, sistemas de segurança, plataformas digitais e ferramentas de autenticação de maneira cada vez mais precisa e eficiente.

Com isso, o reconhecimento facial evoluiu para uma tecnologia capaz de operar em larga escala, oferecendo rapidez e alto desempenho. No entanto, seu funcionamento técnico complexo exige análises cuidadosas sobre seus impactos sociais, especialmente em relação a privacidade, vieses e uso ético,



aspectos fundamentais para compreender suas implicações no cenário contemporâneo da inteligência artificial.

3.3 AVANÇOS RECENTES

Os avanços recentes no reconhecimento facial refletem a rápida evolução da visão computacional impulsionada pelo deep learning, resultando em sistemas cada vez mais precisos, eficientes e amplamente difundidos no cotidiano. Um dos progressos mais significativos diz respeito ao aumento contínuo da acurácia dos modelos. Graças às redes neurais profundas e ao uso de grandes conjuntos de dados, os sistemas atuais são capazes de operar com taxas de erro extremamente baixas, aproximando-se — e em alguns contextos superando — a capacidade humana de identificar rostos. Segundo Taigman et al. (2014), o desenvolvimento de arquiteturas mais robustas, aliadas a técnicas como *data augmentation* e aprendizado contrastivo, contribuiu para a construção de modelos capazes de reconhecer indivíduos mesmo sob condições adversas, como variações de iluminação, ângulos diferentes e mudanças na expressão facial.

Outro avanço importante está relacionado à implementação dessas tecnologias em dispositivos móveis. A popularização de sistemas como o Face ID, presente nos smartphones da Apple, demonstra a maturidade alcançada pela tecnologia ao permitir que a autenticação facial seja utilizada de forma segura e rápida em milhões de dispositivos. Esses sistemas utilizam sensores infravermelhos, câmeras de profundidade e modelos de deep learning integrados ao hardware, garantindo alto desempenho mesmo com restrições de energia e processamento. Conforme Kwon et al. (2021) destacam, a integração entre hardware especializado (como chips neurais) e algoritmos avançados tornou possível realizar reconhecimento facial em tempo real diretamente no dispositivo, preservando privacidade ao evitar o envio de dados biométricos para servidores externos.

Além disso, o uso do reconhecimento facial se expandiu de maneira expressiva nas plataformas digitais. Aplicativos de redes sociais e serviços de vídeo, como Instagram, TikTok e Snapchat, utilizam modelos de visão computacional para aplicar filtros faciais, realizar mapeamento de expressão e criar efeitos interativos complexos. Nesses contextos, a tecnologia não é apenas funcional, mas também parte da experiência estética e do entretenimento, mostrando como a IA se tornou acessível ao usuário comum. Paralelamente, sistemas de controle de acesso em ambientes corporativos, aeroportos e espaços públicos têm adotado algoritmos avançados de identificação para substituir cartões, senhas e documentos físicos, ampliando a eficiência e a segurança operacionais.

Outro ponto fundamental no avanço da área é o surgimento e a popularização de modelos de deep learning pré-treinados. Redes como VGGFace2, FaceNet e ArcFace foram treinadas em milhões de imagens e disponibilizadas para pesquisadores e desenvolvedores, democratizando o acesso a tecnologias de ponta. Esses modelos pré-treinados reduzem significativamente o tempo e os recursos necessários para

construir sistemas de reconhecimento facial, permitindo que empresas e pesquisadores adaptem as arquiteturas a suas necessidades específicas sem a necessidade de treinar uma rede do zero. Como observam Deng et al. (2019), essa abordagem favorece o desenvolvimento de soluções mais robustas e eficientes, contribuindo para a rápida evolução e disseminação da tecnologia.

Dessa forma, os avanços recentes no reconhecimento facial demonstram não apenas o amadurecimento técnico da área, mas também sua crescente inserção na vida cotidiana, reforçando a necessidade de debates éticos e regulatórios diante de seu uso cada vez mais sofisticado e abrangente.

3.4 RISCOS E DESAFIOS

Os riscos e desafios associados ao reconhecimento facial acompanham a rápida expansão dessa tecnologia e revelam questões éticas, técnicas e sociais que não podem ser ignoradas. Um dos principais problemas diz respeito à privacidade e à proteção de dados biométricos. Diferentemente de uma senha ou cartão, a face é um identificador único e permanente, não podendo ser “trocada” caso seja violada. Segundo Zuboff (2019), tecnologias que capturam e analisam dados humanos sensíveis ampliam significativamente as formas de vigilância e exploração, tornando urgente a discussão sobre consentimento, segurança e limites no uso de informações biométricas. A Lei Geral de Proteção de Dados (LGPD) no Brasil classifica dados biométricos como sensíveis, reforçando que seu uso exige justificativa, necessidade e proteção reforçada.

Outro risco importante é o da vigilância massiva e da perda de anonimato em espaços públicos. Sistemas de câmeras integrados a algoritmos de reconhecimento facial permitem identificar pessoas em multidões, rastrear deslocamentos e reconstruir padrões de comportamento. Lyon (2018) destaca que tais sistemas, quando utilizados sem transparência e regulação, ampliam o poder de vigilância dos agentes estatais e corporativos, criando um ambiente de monitoramento constante. Essa situação pode gerar efeitos nocivos à democracia, à liberdade de expressão e ao direito de ir e vir, especialmente quando a tecnologia é usada para controle social ou repressão política. Os vieses algorítmicos representam outro desafio grave. Diversas pesquisas demonstram que sistemas de reconhecimento facial apresentam taxas de erro significativamente maiores para mulheres, pessoas negras e outras minorias. O estudo de Buolamwini e Gebru (2018), realizado no MIT, evidenciou que sistemas comerciais apresentavam acurácia acima de 99% para homens brancos, mas índices alarmantes de falhas ao identificar mulheres negras. Esses resultados mostram que a tecnologia pode reforçar desigualdades históricas, gerar discriminação institucional e comprometer a equidade em aplicações como policiamento, controle de fronteiras ou recrutamento.

O uso indevido da tecnologia por governos ou empresas também constitui uma preocupação crescente. Em contextos autoritários, o reconhecimento facial pode ser empregado para monitorar opositores políticos, jornalistas ou grupos vulneráveis, aumentando riscos de perseguição e repressão. No setor privado, seu uso sem consentimento pode alimentar práticas abusivas, como rastreamento de

consumidores, coleta oculta de dados ou aplicações inadequadas em ambientes laborais. Como aponta O’Neil (2016), sistemas algorítmicos mal regulados tendem a operar como “armas de destruição matemática”, afetando indivíduos de forma invisível e sem mecanismos de contestação.

Por fim, há vulnerabilidades técnicas que desafiam a confiabilidade desses sistemas. Deepfakes — vídeos gerados por IA capazes de reproduzir fielmente o rosto de uma pessoa — representam uma ameaça à segurança digital, podendo ser usados para fraudes, chantagens, manipulação de opinião pública ou usurpação de identidade. Da mesma forma, ataques de *spoofing*, como o uso de máscaras 3D, fotos impressas ou projeções, podem enganar sistemas de reconhecimento facial, demonstrando que nem sempre esses mecanismos são infalíveis. Conforme relata Tolosana et al. (2020), técnicas de falsificação facial evoluem rapidamente, exigindo a criação de defesas robustas e atualizadas.

Diante desses riscos, torna-se fundamental que o desenvolvimento e o uso de tecnologias de reconhecimento facial sejam acompanhados de políticas claras, fiscalização eficaz e reflexão ética. A busca por inovação deve caminhar junto à proteção dos direitos fundamentais, garantindo que os avanços tecnológicos não se convertam em instrumentos de violação de liberdades individuais e coletivas.

4 CONCLUSÃO

O estudo permitiu compreender que a visão computacional aplicada ao reconhecimento facial representa um dos avanços mais significativos da inteligência artificial contemporânea, reunindo técnicas sofisticadas de aprendizado profundo, grandes bases de dados e crescente capacidade computacional para realizar tarefas antes exclusivas da percepção humana. A análise demonstrou que, do ponto de vista técnico, a tecnologia evoluiu de maneira expressiva nas últimas décadas, alcançando altos índices de precisão e tornando-se amplamente utilizada em dispositivos móveis, plataformas digitais, sistemas de autenticação e mecanismos de vigilância. Essa expansão foi impulsionada por redes neurais convolucionais capazes de extrair características faciais de forma altamente eficiente, produzindo embeddings robustos e comparáveis com rapidez e confiabilidade em diferentes contextos de uso.

Entretanto, apesar de seus avanços, o reconhecimento facial também se mostrou uma tecnologia marcada por riscos significativos que precisam ser considerados de maneira crítica. Os problemas relacionados à privacidade e ao tratamento de dados biométricos revelaram-se centrais, já que o rosto é um identificador permanente, sensível e impossível de substituir em caso de vazamento ou uso indevido. A pesquisa também evidenciou que sistemas dessa natureza ampliam as possibilidades de vigilância e monitoramento em larga escala, ameaçando direitos fundamentais como anonimato e liberdade de circulação, especialmente em ambientes públicos e em sociedades com pouca transparência na atuação de instituições governamentais e corporativas.

Além disso, os vieses algorítmicos identificados na literatura reforçaram a necessidade de cautela,



pois demonstraram que mulheres, negros e outras minorias continuam enfrentando maiores taxas de erro no reconhecimento facial, o que pode resultar em discriminação institucional, injustiças em sistemas de segurança e desigualdades reforçadas por meio de decisões automatizadas. Também se constatou que a tecnologia está sujeita a vulnerabilidades técnicas, como *deepfakes* e ataques de *spoofing*, capazes de burlar mecanismos de autenticação e comprometer a confiabilidade de sistemas que dependem exclusivamente da identificação facial.

Dessa forma, o trabalho concluiu que, embora o reconhecimento facial represente um marco na evolução da inteligência artificial e ofereça inúmeros benefícios em termos de praticidade, segurança e automação, seu uso deve ser acompanhado de regulamentações claras, fiscalização constante e políticas que assegurem transparência, equidade e proteção de dados sensíveis. A análise evidenciou que a adoção dessa tecnologia só pode ser considerada socialmente responsável quando se estabelece um equilíbrio entre inovação e direitos fundamentais, evitando que avanços técnicos se convertam em instrumentos de vigilância abusiva ou discriminação. Assim, destaca-se a importância de que governos, empresas e sociedade civil atuem de forma conjunta na construção de diretrizes éticas, mecanismos de controle e práticas de desenvolvimento seguro, garantindo que o reconhecimento facial seja aplicado de maneira justa, confiável e alinhada aos valores democráticos.



REFERÊNCIAS BIBLIOGRÁFICAS

- BOJANOWSKI, Piotr; JOULIN, Armand. Unsupervised learning by predicting noise. International Conference on Machine Learning, 2017.
- BUOLAMWINI, Joy; GEBRU, Timnit. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. Proceedings of Machine Learning Research, 2018.
- DENG, Jiankang et al. ArcFace: Additive Angular Margin Loss for Deep Face Recognition. IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2019.
- GONZALEZ, Rafael C.; WOODS, Richard E. Digital Image Processing. 4. ed. Pearson, 2018.
- GOODFELLOW, Ian; BENGIO, Yoshua; COURVILLE, Aaron. Deep Learning. MIT Press, 2016.
- KWON, Jisun et al. On-device deep neural networks and their applications on mobile phones. IEEE Transactions on Mobile Computing, 2021.
- LECUN, Yann; BENGIO, Yoshua; HINTON, Geoffrey. Deep learning. Nature, v. 521, p. 436–444, 2015.
- LYON, David. The Culture of Surveillance. Polity Press, 2018. O'NEIL, Cathy. Weapons of Math Destruction. Crown, 2016.
- SCHROFF, Florian; KALENICHENKO, Dmitry; PHILBIN, James. FaceNet: A unified embedding for face recognition and clustering. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2015.
- SZELISKI, Richard. Computer Vision: Algorithms and Applications. 2. ed. Springer, 2022.
- TAIGMAN, Yaniv et al. DeepFace: Closing the Gap to Human-Level Performance in Face Verification. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2014.
- TOLOSANA, Ruben et al. DeepFakes and Beyond: A Survey of Face Manipulation and Fake Detection. Information Fusion, 2020.
- VIOLA, Paul; JONES, Michael. Rapid object detection using a boosted cascade of simple features. IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 2001.
- ZHAO, Wenyi et al. Face recognition: A literature survey. ACM Computing Surveys, v. 35, n. 4, p. 399–458, 2003.
- ZUBOFF, Shoshana. The Age of Surveillance Capitalism. PublicAffairs, 2019.