ESCOLA SUPERIOR DE GUERRA

GEORGE WASHINGTON MENEZES

A AÇÃO DO USO DA INTELIGÊNCIA ARTIFICIAL E MICROFEIÇÕES FACIAIS PARA MITIGAR OS RISCOS DE *DEEPFAKES* PARA A AUTENTICAÇÃO POR BIOMETRIA FACIAL NO SETOR FINANCEIRO BRASILIERO

Trabalho Acadêmico – Ensaio Acadêmico apresentado ao Departamento de Estudos da Escola Superior de Guerra como requisito à obtenção do certificado do Curso Superior de Segurança e Defesa Cibernética.

Orientador: Prof. Ricardo Alves Neiva

Rio de Janeiro

2024

C2024 ESG

Documento assinado digitalmente
gov.br
GEORGE WASHINGTON MENEZES
Data: 17/10/2024 21:12:36-0300
Verifique em https://validar.iti.gov.br

GEORGE WASHINGTON MENEZES

RESUMO

O setor bancário Brasileiro se transformou na última década com a migração dos clientes para canais digitais, a chamada “Transformação Digital”. Dois marcos recentes importantes foi, o primeiro, a liberação pelo Banco Central para o funcionamento dos bancos nativamente digitais, que já nascem sem agência física. O segundo, os efeitos da pandemia que aceleram a digitalização em todos os setores e ao mesmo tempo incluíram 38 milhões de pessoas no setor. Por ser um setor sustentado pela confiança, a segurança cibernética é fator determinante para solvência das instituições. A biometria facial é uma poderosa solução para garantir a autenticidade dos clientes. Contudo, o avanço da Inteligência Artificial desta década coloca desafios adicionais para o uso da autenticação biométrica. Em paralelo temos uma crescente tensão geopolítica que coloca o Brasil em posição sensível e potencial alvo de ciberataques. Essa conjuntura pode gerar pressões adicionais sobre a segurança financeira, tornando ainda mais urgente o desenvolvimento de soluções tecnológicas nacionais para proteger o setor financeiro brasileiro contra-ataques cibernéticos e fraudes. O ensaio ressalta a importância da colaboração entre governo, setor privado e academia na criação de tecnologias nacionais de segurança robustas, que podem aumentar o grau de segurança do setor financeiro e ser estendidas para as demais infraestruturas críticas.

Palavras-chave: biometria facial; microexpressões faciais; segurança nacional; inteligência artificial.

ABSTRACT

The Brazilian banking sector has undergone significant transformation over the past decade, driven by the migration of clients to digital channels, a process known as Digital Transformation. Two recent milestones are noteworthy. First, the Central Bank's authorization of native digital banks, which operate without physical branches. Second, the pandemic accelerated digitalization across all sectors, integrating 38 million new clients into the banking system. Trust underpins this sector, making cybersecurity a crucial factor for institutional solvency. Facial biometrics has emerged as a powerful tool for ensuring client authenticity. However, the rapid advancements in Artificial Intelligence this decade present additional challenges for biometric authentication. Concurrently, rising geopolitical tensions place Brazil in a vulnerable position, as a potential target for cyberattacks. This scenario could exert additional pressure on financial security, highlighting the urgency of developing national technological solutions to safeguard the Brazilian financial sector from cyberattacks and fraud. The essay underscores the importance of collaboration between government, private sector, and academia to develop robust national security technologies, which can not only enhance the security of the financial sector but also be extended to other critical infrastructures.

***Keywords**: facial biometrics; microexpressions; national security; deepfakes; artificial intelligence*

1 INTRODUÇÃO

Em 23 dez 2023 o Governo Federal editou o decreto n° 11.856 que Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança com o objetivo de orientar a atividade de segurança cibernética no País (Brasil, 2023). No seu 2º artigo, no inciso III, o decreto define como princípio, dentre outros, “a prevenção de incidentes e de ataques cibernéticos, em particular aqueles dirigidos a infraestruturas críticas nacionais e a serviços essenciais prestados à sociedade”.

Anteriormente, em dez 2020, havia sido editado o decreto nº 10.569 aprovando a Estratégia Nacional de Segurança de Infraestruturas Críticas. No Anexo desse mesmo decreto, já na introdução, o decreto define:

> As infraestruturas de comunicações, de energia, de transportes, de finanças e de águas, entre outras, possuem dimensão estratégica, uma vez que desempenham papel essencial tanto para a segurança e soberania nacionais, como para a integração e o desenvolvimento econômico sustentável do País. Fatores que prejudiquem o adequado fornecimento dos serviços provenientes dessas infraestruturas podem acarretar transtornos e prejuízos ao Estado, à sociedade e ao meio ambiente (Brasil, 2022).

O Banco Central do Brasil (BC), órgão normativo e supervisor do Sistema Financeiro Nacional (SFN), delegação recebida por meio da Lei nº 4595 de 31 dez 1964, que dispõe sobre a política e as instituições financeiras, implementou a Resolução CMN nº 4.893, de 26 de fev de 2021, na qual define no seu Art. 1º:

> Esta Resolução dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil (Banco Central do Brasil, 2021).

E específica em seu At. 2º:

> Art. 2º As instituições referidas no art. 1º devem implementar e manter política de segurança cibernética formulada com base em princípios e diretrizes que busquem assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados (Banco Central do Brasil, 2021).

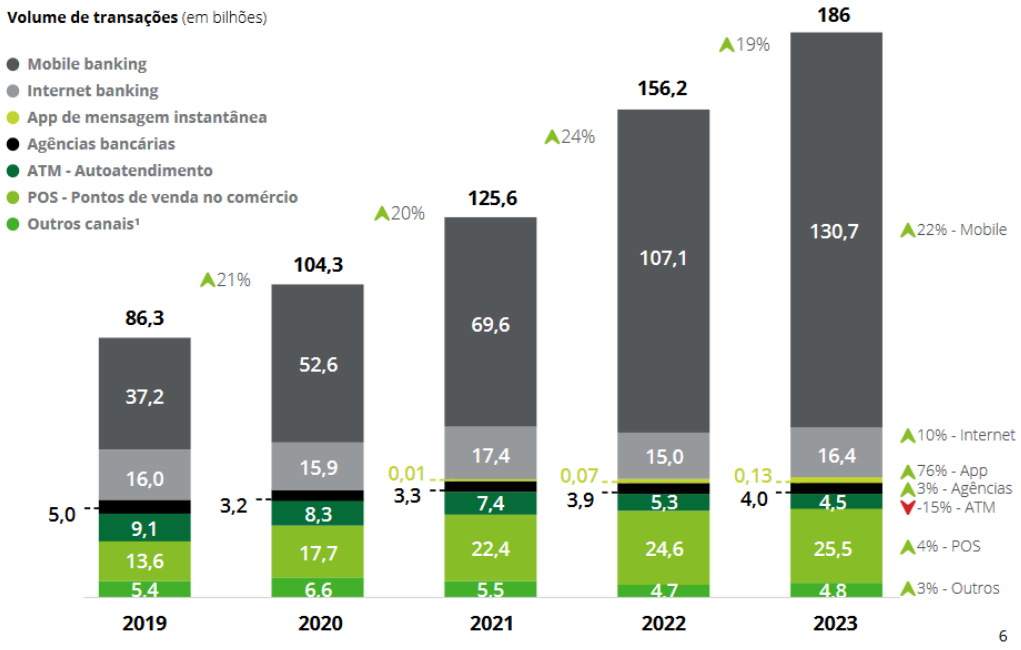
Portanto, a segurança do setor bancário, além das obrigações das instituições com seus clientes definidas pelo Supervisor, também é considerada uma questão de Segurança Nacional, uma vez que se trata de infraestrutura críticas.

Considerado um dos sistemas mais avançados e automatizados entre os países desenvolvidos e em desenvolvimento, o Sistema Financeiro Nacional, em especial o setor bancário, apresentou evolução tecnológica significativa nos últimos 20 anos.

Após a pandemia de 2020/2021, houve sensível crescimento na bancarização de segmento da população que se encontrava à margem do sistema. No período foram incluídos no sistema financeiro cerca de 38 milhões de brasileiros (Federação Brasileira de Bancos, 2024)

O estudo da FEBRABAN afirma ainda que, em 2023, 7 em cada 10 transações financeiras foram realizadas por meio de celular. Além disso, houve um aumento de 19% no número de transações em relação 2022. Retrocedendo ao ano de 2019, pré pandemia, o aumento em relação a 2023 chega a 116% (Federação Brasileira de Bancos, 2024).

Figura 1 – Evolução do uso de *mobile banking* entre 2019 e 2023



Fonte: Federação Brasileira de Bancos, 2024.

Conforme o mesmo relatório (Federação Brasileira de Bancos, 2024), 72% dos usuários do *mobile banking* são considerados *heavy users*, ou seja, são usuários que realizaram mais de 80% das suas transações nesse canal nos últimos três meses.

Todo esse movimento de digitalização no setor é denominado Transformação Digital do Setor Financeiro, que se acelerou a partir do momento que o Banco Central autorizou o funcionamento das *fintechs*, depois denominadas bancos digitais, que já nasceram sem pontos de presença físicos.

> Bancos ao redor do mundo têm percebido que investimentos em tecnologias digitais são formas de beneficiar a aquisição de novos clientes, bem como conquistar a satisfação. O setor bancário busca o desenvolvimento de melhorias de suas capacidades digitais em atividades *front office* e, para

> muitas instituições de varejo, os canais virtuais e móveis se tornaram tão importantes quanto agências e caixas eletrônicos. Nesse contexto, destacam-se as *fintechs* que oferecem serviços de conta e de cartão. Players em grande ascensão, eles forçam as instituições tradicionais a se revolucionarem, contribuindo, assim, para a transformação digital do sistema como um todo (Feitosa, 2020).

Além da segurança nas transações bancárias, que é o primeiro aspecto que vem à mente quando se fala em segurança nos bancos, a proteção aos demais dados dos clientes que os bancos têm em custódia tem mesma importância. Informações de crédito, cadastro, histórico bancário, renda e patrimônio, situação fiscal, entre outras, são também sensíveis, e acessos indevidos podem gerar prejuízos e riscos para seus clientes. Essa obrigação sempre esteve presente nas avaliações de riscos das instituições, no entanto, após a edição da Lei nº 13.709, de 14 agosto de 2018 (Brasil, 2018), conhecida como Lei da LGPD, outras responsabilidades foram acrescentadas, incluindo penalidades severas em casos de acesso indevido às informações individuais de cada cliente.

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios (Brasil, 2018).

A transformação digital, que por um lado traz conforto e acessibilidade para os clientes, por outro, apresenta um grande desafio para que as instituições financeiras garantam a segurança em todas as suas vertentes, mantendo inabalável a confiança no Sistema Financeiro Nacional.

A América Latina e, em especial, o Brasil, são alvos importantes de tentativas de ataques cibernéticos em relação ao mundo, mesmo quando comparado com os países do Norte que possuem número superior de sites de acesso. O Relatório da empresa Akamai, especialista em proteção tecnológica afirma que:

> Embora a EMEA supere a maioria das regiões em número de domínios suspeitos e visitas a páginas, a APJ tem a pontuação média de ameaça mais alta: 97. A América Latina, apesar de ter o número mais baixo de visitas a sites, recebe uma pontuação média surpreendente de ameaça de 94. Isso indica que os consumidores tanto na América Latina quanto na APJ correm um risco maior de ter suas informações bancárias e outros dados confidenciais roubados ao visitar sites (Akamai, 2024).

A evolução de soluções de autenticação de clientes é um recorte especial neste cenário. Soluções baseadas em códigos e senhas há muito tempo não são

suficientes para garantir a confiabilidade de autenticação, desde a abertura de relacionamento do cliente com a instituição financeira até na movimentação de valores mais substanciais.

As boas práticas atuais recomendam que se adote a chamada autenticação multifator, levando-se em consideração uma informação que o cliente sabe (ex: senha), algo que o cliente tem (ex.: *token*) e algo que ele é. Neste último, destacam-se as soluções de biometria.

> Mecanismos de autenticação se baseiam em três paradigmas: algo-que-você-sabe (senha de acesso, por exemplo), algo-que-você-tem (chaves, cartões de acesso e chaves criptográficas, por exemplo) ou algo-que-você-é (voz, impressão digital, retina, palma da mão e qualquer outra) (Maziero, 2019, p. 371).

Inicialmente essas soluções estavam restritas ao uso da biometria da digital. Com a evolução das tecnologias, hoje podemos utilizar também as biometrias faciais, por íris, voz, retina, digitação, dentre outras.

No setor bancário, há crescente uso da biometria facial por oferecer vantagens como rapidez, conveniência e a eliminação de ações acessórias para identificação. Paralelamente a evolução das soluções de segurança com os avanços tecnológicos, avançam também a capacidade de burla pelos cibercriminosos.

No caso da biometria facial, o crescimento da Inteligência Artificial, em especial o subcampo da *deep learrning*, nesse mesmo período, trouxe potencial risco com o desenvolvimento das *deepfake*s. O termo *deepfake* refere-se a mídias falsificadas geradas por redes neurais profundas nas quais imagens ou sons capturados de determinadas pessoas são substituídos pelos de outras por meio de técnicas avançadas com a finalidade de manipular conteúdo visuais e/ou sonoros, com enorme potencial de falseamento da realidade (Fanaya, 2021).

Os *deepfake*s são capazes de criar imitações convincentes de rostos e vozes, o que levanta preocupações sobre a vulnerabilidade dos sistemas de reconhecimento facial. Esses vídeos podem ser usados por fraudadores para simular a identidade de clientes e obter acesso indevido a suas contas.

> Um *deepfake* é um conteúdo gerado por uma inteligência artificial que é autêntico aos olhos de um ser humano. A palavra *deepfake* é uma combinação das palavras ‘aprendizado profundo’ e ‘falso’ e refere-se principalmente ao conteúdo gerado por uma rede neural artificial, um ramo do aprendizado de máquina. Por exemplo, dublagem de vídeos realistas de filmes estrangeiros, educação por meio da reanimação de figuras históricas, e experimentação virtual de roupas durante as compras (Mirsky; Lee, 2016).

As equipes de segurança implementaram soluções complementares para a mitigação do uso *deepfake*s, com a inclusão de rotinas de "*liveness*" (prova de vida), como a solicitação de piscadas ou movimentos de cabeça. Essas medidas, porém, reduzem a naturalidade do uso de biometria facial pelos clientes, pois exigem interações adicionais não comuns no cotidiano.

Diante do avanço dessas ameaças, surge a necessidade de soluções de autenticação ainda mais robustas. Este ensaio propõe o uso de microexpressões faciais, combinadas a técnicas de *deep learrning*, como uma solução potencial para aumentar a segurança dos sistemas bancários. As microexpressões, por serem sutis e involuntárias, apresentam características que são difíceis de replicar, até mesmo por tecnologias de *deepfake*s, tornando-se uma camada adicional de segurança.

O objetivo desse trabalho é explorar o conceito de microexpressões faciais e discutir a viabilidade de sua implementação como uma forma de autenticação segura e resistente à *deepfakes*, o que poderia representar uma solução estratégica para diversos desafios de segurança do Estado, das forças de defesa, das forças de segurança públicas e da iniciativa privada, incluindo a mitigação dos riscos de fraude e acessos indevidos em sistemas bancários (Souza, 2020).

2 REFERENCIAL TEÓRICO

Os sistemas de autenticação biométrica têm crescido à medida que a tecnologia se torna mais confiável e acessível, como uma forma eficiente e segura de verificar a identidade das pessoas. No setor bancário é amplamente utilizada para autenticar acesso a contas e realizar transações sensíveis, como transferências e pagamentos.

> O termo Biometria refere-se ao reconhecimento automatizado de indivíduos baseado em suas caraterísticas de comportamento ou biológicas. Consiste na associação de métodos estatísticos com as características físicas ou de comportamento para a identificação do indivíduo. Para tanto, são mensuradas características físicas, como a cor dos olhos, a voz, a textura da íris, o formato do rosto, as impressões digitais ou comportamentais, como a forma de andar ou de falar, entre outras. Essas características possuem como princípio serem únicas para cada indivíduo (Souza, 2020).

2.1 Aderência do tema aos propósitos da Escola Superior de Guerra

A Escola Superior de Guerra (ESG), criada pela Lei nº 785, de 20 de agosto de 1949, integra a estrutura do Ministério da Defesa (MD), sendo estabelecida como um Instituto de Altos Estudos. Sua missão é: "*Desenvolver e disseminar os conhecimentos de Defesa, Segurança e Desenvolvimento Nacional, com o propósito*

de capacitar civis e militares para o planejamento e o exercício das funções de direção e assessoramento, bem como de ampliar o envolvimento da sociedade brasileira nos assuntos de Defesa Nacional", portanto, é imprescindível que os assuntos discutidos sejam de cunho estratégicos e de interesse nacional (Escola Superior de Guerra, 2023).

A busca de solução de identificação em tempo real que seja imune às *deepfake*s se enquadram nesta categoria. A tecnologia, que está em constante desenvolvimento, permite simular imagens, sons e movimentos, utilizando-se técnicas de Inteligência Artificial, de difícil identificação por humanos e mesmo por técnicas digitais tradicionais. O uso de *deepfake* pode fragilizar os mecanismos de acesso a instalações de alto nível de segurança, o acesso a sistemas sensíveis e estratégicos, causar distúrbios sociais com a divulgação de notícias falsas e corromper o resultado de eleições democráticas.

Como já mencionado na introdução, o setor financeiro faz parte do conjunto de infraestruturas críticas do Estado. E mais especificamente, a opção de usarmos o setor bancário neste estudo deve-se a dois fatores: o primeiro, é que um ataque massivo ao setor, quer seja a uma instituição ou ao sistema, que tivesse êxito no acesso a grande número de contas de clientes tem o potencial de trazer considerável prejuízo financeiro, pois a biometria facial é responsável pela liberação de transações mais sensíveis e de maior valor. Mas para além disso, pior que o prejuízo financeiro, poderia expor publicamente dados sensíveis, como demonstrativos financeiros de clientes, o que colocaria em dúvida a segurança bancária e consequentemente aumento o risco sistêmico.

> A expressão risco sistêmica não é muito precisa. Frequentemente, ela se refere ao fenômeno do contágio, isto é, de que instituições bancárias ‘doentes’ podem acabar fazendo com que outras instituições, em si saudáveis, acabem se tornando também doentes. Assim, é possível conceber-se que pressões sobre um banco individual possam acabar se tornando um fator de crise para todo o sistema bancário. Por outro lado, em seu mais frequente, a expressão risco sistêmica designa o contágio não apenas para todo o setor bancário, mas, na verdade, para toda a economia (Carvalho, 2020).

Em um cenário hipotético de um ataque cibernético planejado, originado em um Estado com interesses conflitantes ou uma organização a mando desse, de significativa intensidade e com o objetivo de enfraquecer o aparato estatal, iniciando com a contaminação de dispositivos celulares de clientes ao longo do tempo, com a apropriação de informações cadastrais de clientes disponíveis na *dark web* e suas

respectivas biometria facial a partir de fotos e vídeos retiradas das redes sociais e tratadas por tecnologias de *deepfake*.

Tal ofensiva poderia, em última instância, permitir o acesso a milhares de aplicativos bancários, que mesmo que não permita operações financeiras, pois normalmente existem camadas adicionais para movimentações financeiras, daria acesso a informações sensíveis, que se divulgadas em massa, abalaria a confiança do sistema, e poderia precipitar um colapso do sistema financeiro nacional.

Os clientes recorreriam aos bancos, seja de forma presencial ou virtual, com o intuito de transferir seus ativos para meios considerados mais seguros, como moedas estrangeiras, depósitos internacionais ou até mesmo valores em espécie.

O que evitaria essa situação extrema seria a resiliência dos sistemas de segurança dos bancos, neste caso especial, sua capacidade de identificar e repudiar os ataques de *deepfakes*.

> A extensão do alcance de um evento sistêmico forte pode ser caracterizada conforme as visões horizontal e vertical do risco sistêmico. A visão horizontal enfoca os eventos e seus desdobramentos de forma circunscrita ao sistema financeiro, isto é, as falências das instituições financeiras e os colapsos dos mercados financeiros. Já a visão vertical transpassa as fronteiras do sistema financeiro e se preocupa com o comportamento da economia como um todo, envolvendo os efeitos de tais eventos sobre a atividade econômica, o investimento, dentre outros aspectos macroeconômicos (Carvalho, 2020).

No Relatório de Estabilidade Financeira Global, publicado em abril de 2024, o Fundo Monetário Internacional (FMI) demonstrou crescente preocupação com os impactos que os ciberataques podem trazer para a estabilidade do setor financeiro mundial.

> Os riscos cibernéticos representam uma ameaça crescente à estabilidade financeira. Incidentes cibernéticos, particularmente de natureza maliciosa, estão se tornando mais frequentes globalmente. A análise neste capítulo mostra que as perdas decorrentes de incidentes cibernéticos têm sido, em geral, modestas no passado, mas podem ser extremas em alguns casos. Embora o setor financeiro ainda não tenha experimentado um ataque cibernético sistêmico — o que sugere que a cibersegurança nas instituições financeiras tem sido adequada aos níveis de ameaça anteriores — os riscos aumentaram substancialmente, devido à crescente digitalização, evolução tecnológica e tensões geopolíticas. Incidentes cibernéticos agora representam uma ameaça aguda à estabilidade macrofinanceira, dado que o setor é caracterizado pela exposição a dados sensíveis, altos níveis de concentração e forte interconectividade — incluindo com a economia real (Fundo Monetário Internacional, 2024).

Dentre as instabilidades geopolíticas diretamente relacionada ao setor financeiro, podemos citar a criação da moeda cambial pelo bloco denominado BRICS, onde o Brasil é um dos sócios fundadores, juntamente com a Rússia, Índia e África do

Sul. Esta moeda que, entraria em competição com o dólar, é vista com ressalvas pelos EUA por afrontar a hegemonia da moeda norte-americana, podendo causar desvalorização da moeda americana e outras consequências econômicas nos EUA.

Não se trata apenas de um fato econômico. O fim do dólar como reserva mundial pode desencadear uma mudança estrutural muito mais severa da geopolítica. O dólar não é somente moeda, é arma de dominação hegemônica e motivo para que os países protagonistas desta transformação possam ser alvos de ações legais ou não, com o objetivo de desestabilizar suas economias, dificultando o projeto de afastamento gradual do dólar.

> No início da década de 2000, o governo dos EUA percebeu que poderia usar o dólar americano como uma arma poderosa contra os adversários, o que acabou por encorajar o desenvolvimento de instituições financeiras globais paralelas pelas nações do BRICS. As sanções financeiras sem precedentes impostas pelos EUA e pela União Europeia (UE) contra a Rússia em resposta à invasão da Ucrânia em fev de 2022 podem ter corroído ainda mais a atratividade global do dólar americano como moeda de reserva mundial. Se, ou quando, houvesse uma alternativa viável ao dólar, o valor do dólar diminuiria, tornando muito menos acessível para os EUA manter militarmente uma presença global e funcional como polícia global. A consequência será o surgimento de uma nova ordem multipolar (Krishnan; Kassa, 2023).

Além da moeda comum do BRICS, vários outros conflitos geopolíticos colocam o Brasil em lados opostos a uma das grandes potências mundiais. No conflito Ucrânia-Rússia, o Brasil se coloca em uma posição de busca de pacificação, sem condenar diretamente a invasão russa, em franca oposição à posição dos EUA e aliados da OTAN. A China não declara apoio à Rússia, mas mantem uma proximidade.

> O Brasil se absteve de condenar diretamente a Rússia, mantendo relações diplomáticas com Moscou e evitando participar de sanções internacionais. Durante uma visita à China em 2023, o presidente Lula criticou a influência de países que fornecem armas, incluindo os EUA, acusando-os de prolongar o conflito. Essa abordagem reforça a posição do Brasil como um ator que busca uma mediação de paz, o que o coloca em oposição à postura mais combativa dos EUA e da OTAN. (Marcondes; Silva, 2023).

No conflito Israel-Palestina-Líbano, o Brasil se posiciona fortemente contrário ao emprego de força desproporcional de Israel, embora condene o ataque do Hamas em out de 2023. Essa posição também colide com o apoio irrestrito americano ao governo israelense.

> No mesmo dia dos terríveis ataques do Hamas contra Israel, o presidente brasileiro Luiz Inácio Lula da Silva foi a público com uma inequívoca. A condenação dos acontecimentos e apresentaram condolências às famílias das vítimas. Ele não condenou um lado ou outro como responsável. Em vez disso, ele prometeu que o Brasil não pouparia esforços para evitar uma escalada e pediu à comunidade internacional que trabalhe para uma retomada imediata das negociações – uma que garanta a existência de um Estado

> palestino economicamente viável coexistindo pacificamente com Israel, com fronteiras seguras para ambos os lados (Kurchin, 2023).

Na agenda de sustentabilidade e transição energética, que na essência é uma discussão das bases econômicas de desenvolvimento mundial, o atual Governo brasileiro quer se posicionar como líder na transição energética sustentável. Esta posição entra em conflito com a China, maior poluidor do mundo. A União Europeia, depois do conflito com a Ucrânia, reduziu suas restrições à produção de energia não renovável. A Rússia, que não participa desta discussão, é um dos maiores exportadores de gás natural, carvão e petróleo conjugado. A matriz energética americana caminha muito lentamente para uma sustentabilidade, e a cada eleição presidencial é tema de amplo debate.

Portanto, o Brasil não tem neste momento um aliado importante no cenário mundial.

> Segundo um novo relatório do Fórum Econômico Mundial, publicado hoje, a transição energética global para um sistema mais equitativo, seguro e sustentável ainda está avançando, mas perdeu força diante do aumento da incerteza mundial. Apesar de 107 dos 120 países analisados no relatório terem demonstrado avanços em suas trajetórias de transição energética na última década, o ritmo global da transição desacelerou, e equilibrar suas diferentes facetas ainda é um desafio significativo. A volatilidade econômica, as tensões geopolíticas exacerbadas e as mudanças tecnológicas todas tiveram um impacto, complicando seu ritmo e sua trajetória. No entanto, há motivos para otimismo, com o aumento dos investimentos globais em energias renováveis e o crescimento considerável no desempenho da transição energética na África subsaariana na última década (Fórum Econômico Mundial, 2024).

Ademais, no cenário de conflitos geopolíticos, o Brasil apresenta vários interesses conflitantes com as principais nações, o que pode torná-lo alvo de eventuais ataques cibernéticos.

O segundo motivo para escolha do setor bancário é baseado na triplica hélice (Governo, Setor Privado e Academia) para o desenvolvimento de tecnologia nacional. O setor bancário é um grande investidor em tecnologia de segurança e tem capital financeiro e humano disponíveis. Demonstrando-se o valor desta solução, o setor poderia dar o suporte necessário para as pesquisas e o desenvolvimento da tecnologia, além de ser um campo ideal para as etapas de prototipagem, piloto e escalonamento em produção de forma controlada. O desenvolvimento deste projeto poderá dar ao Brasil uma tecnologia nacional, raro no ambiente de segurança

cibernética, que abarcaria as diversas possibilidades de uso da biometria facial para as demais infraestruturas críticas do país.

> Tendo se originado como uma metáfora para identificar os protagonistas de um sistema icônico de inovação regional na Rota 128 em Boston, a Hélice Tríplice tornou-se um modelo reconhecido internacionalmente, que está no âmago da disciplina emergente de estudos de inovação, e um guia de políticas e práticas nos âmbitos local, regional, nacional e multinacional. A Hélice Tríplice provê uma metodologia para examinar pontos fortes e fracos locais e preencher lacunas nas relações entre universidades, indústrias e governos, com vistas a desenvolver uma estratégia de inovação bem-sucedida. Identificar a fonte generativa do desenvolvimento socioeconômico baseado no conhecimento é o cerne do projeto de inovação da Hélice Tríplice para aprimorar as interações universidade-indústria-governo (Etzkowitz, 2017).

Portanto, essas argumentações sustentam o caráter estratégico do tema a ser desenvolvido neste ensaio teórico.

2.2 Evolução da Biometria para reconhecimento Individual

A biometria tem sido vista como uma alternativa mais segura e conveniente para permissão de acessos em comparação aos métodos tradicionais, como senhas e PINs, que podem ser facilmente esquecidos ou comprometidos.

O uso desta tecnologia não é recente. Remonta a antiguidade a sua utilização para identificar pessoas, sendo a biometria de impressão digital a mais conhecida pelo público em geral. O avanço no uso destas soluções se tornou viável nos últimos anos em função da evolução de tecnologias de imagem, processamento, armazenamento e transferência de dados.

> O termo “biometria” é derivado das palavras gregas “bio” (vida) e “métricas” (medir). Sistemas biométricos automatizados só se tornaram disponíveis nas últimas décadas, devido a avanços significativos no campo do processamento de computadores. Muitos de essas novas técnicas automatizadas, no entanto, são baseadas em ideias que foram originalmente concebidos há centenas, até milhares de anos atrás (Blackburn *et al*., 2006).

Dentre as várias opções biométricas já mencionadas, vem ganhando destaque a utilização da biometria facial. A identificação de faces é algo natural para o ser humano. Mais que a voz, é uma característica que utilizamos normalmente para identificar uma pessoa. A face, pela facilidade de arquivamento (fotos e vídeos) e recuperação (ver uma foto), serve inclusive de repositório de memórias.

E essa identificação se mantem mesmo com o passar dos anos e as alterações decorrentes idade, o que faz dela uma opção natural e poderosa para os sistemas atuais de segurança. Pela facilidade de captura, com as câmeras, até mesmo de celulares, em ambientes públicos e privados, é possível, resguardadas as questões de

proteção dos dados individuais, implementar sistemas de acesso ao ambiente de trabalho, a identificação em alfândegas, entrada em eventos públicos, e privados com controle de acesso, acessos a sistemas computacionais, identificação de criminosos procurados, pessoas desaparecidas, dentre várias outras possibilidades.

> Nos últimos anos, o método biométrico de reconhecimento facial, tem ganhado atenção significativa, haja vista os bons resultados obtidos, seja em análises de imagens estáticas ou em vídeos, bidimensionais (2D) ou tridimensionais (3D) e utilizam-se de métodos estatísticos de análise de componentes principais (PCA), redes neurais artificiais, entre outros para o reconhecimento das caraterísticas locais como olhos, nariz e boca, por meio de métodos de correspondência de gráficos e de métodos híbridos (combinando os dois últimos) para caracterizar um indivíduo (Souza, 2020).

Tabela 1 - Comparação entre os vários tipos de biometrias quanto a custo e performance (H = *High*; M = *Medium*; L = *Low*)

Tipo de biometria	Unicidade	Complexidade	Universalidade	Quantificavel	Desempenho	Comparavel	Capacidade coleta	Aceitação	Custo	Uso
Digital	M	L	H	H	M	H	H	H	M	H
Iris	H	M	H	H	H	H	H	H	H	M
Facial	M	M	H	H	M	M	H	H	M	M
Palma Mão	M	H	H	H	M	M	L	L	H	M
Orelha	M	H	H	H	L	L	L	L	H	L
Pegada	M	H	M	M	L	L	L	L	H	L
Veia do Dedo	H	H	H	L	H	H	L	L	H	L
Voz	M	H	H	M	M	M	L	L	H	L
Assinatura	L	H	H	H	L	L	M	H	L	L
Teclado	L	M	M	L	L	L	L	L	H	L

Fonte: Rousan; Intrigila, 2020.

Analisando a Tabela 1, vê-se que todos os métodos têm vantagens e desvantagens. Para o uso em larga escala, como para os clientes de um banco, a Biometria Facial pode ser considerada a melhor opção. Não apresentou nenhum item classificado como "*Low*". Também, para os itens em que ela foi considerada "*Medium*": individualização, complexidade, comparação, custo e uso, já poderiam ser reclassificados para "*high*" conforme será demonstrado neste artigo, em função do grande avanço da Inteligência Artificial, principalmente do uso de *deep Learning*, e do uso massivo de aparelhos celulares de média resolução pelos clientes do sistema financeiro nacional.

Porém, como todo sistema de segurança tecnológico, a biometria facial não está imune à tentativa de fraudes e cibercrimes. Há a necessidade de avanços constantes na tecnologia para que se mantenha confiável e segura.

> Para combater as crescentes ameaças à segurança e a fraude financeira, e para facilitar a personalização e a conveniência, a importância do biométricas

> como uma ferramenta confiável para reconhecimento de pessoas foram estabelecidas além de qualquer dúvida. É realmente fascinante que um sistema possa reconhecer uma pessoa com precisão extremamente alta dentro de uma fração de um segundo com base no padrão de fricção na ponta do dedo, ou os padrões texturais no estroma de sua íris, usando um padrão processador de dados, como um laptop ou um telefone celular. Este é um significativo avanço, dado que o primeiro artigo em biometria automatizada para o reconhecimento foi publicado há apenas 50 anos (Jain; Nandakumar; Ross, 2016).

2.3 *Deepfake*: Conceitos e Ameaças à Segurança dos sistemas Biométricos

As *deepfake*s são manipulações de mídias digitais, em especial voz e imagem de uma pessoa, por meio de Inteligência Artificial, com o objetivo de se passar pela pessoa original, atribuindo-lhes a autoria da mensagem vinculada pela *deepfake*. Tenta-se imitar as características acústicas da voz, as feições e movimentos do rosto para parecer uma imagem real.

> No entanto, apesar das aplicações positivas dos *deepfake*s, a tecnologia é famosa pelos seus aspectos antiéticos e maliciosos. No final de 2017, um usuário do Reddit chamado '*deepfake*s' estava usando aprendizagem profunda para trocar rostos de celebridades em vídeos pornográficos e os publicava online (Mirsky; Lee, 2016).

Essas manipulações estão sendo possíveis em função dos avanços da Inteligência Artificial e drástica redução dos custos com a crescente utilização de soluções em nuvem. A técnica utiliza aprendizado profundo (*deep learrning*), especialmente o uso de Redes Adversariais Generativas (GANs).

São variados os objetivos dos executores dessas imagens falsas. Desde inocentes brincadeiras para satirizar um integrante de um grupo de WhatsApp, passando pela disseminação de notícias falsas que ganham verossimilhança por parecer ser atribuída a pessoa confiável, até que é nosso caso de interesse, a simulação para burlar sistemas de segurança baseados em biometria facial, como as utilizadas em bancos, visando fraude financeira.

> As técnicas de *deepfake* dependem de modelos avançados de aprendizado profundo, como *autoencoders* e redes adversariais generativas (GANs), para analisar as características faciais e comportamentais de uma pessoa, possibilitando a síntese de imagens manipuladas que replicam gestos e movimentos semelhantes. Como os *deepfake*s são gerados usando Redes Adversariais Generativas (GANs) (Waseem, *et al*, 2023).

As Redes Adversarias Generativas (GANs), pressupõe uma interação entre duas redes neurais profundas, em que a primeira, denominada geradora, cria imagens ou vídeos falsos e os submete à segunda rede, denominada discriminadora, que por sua vez tenta identificar se o *input* gerado é falso ou verdadeiro. O aprendizado da

rede é medido para percentual de imagens criadas pela geradora que são aceitos como verdadeiras pela discriminadora.

> As GANs consistem em duas redes neurais competidoras: i) uma rede generativa (G) que captura a distribuição dos dados para gerar amostras sintéticas, e ii) um modelo discriminativo (D) que distingue exemplos reais daqueles gerados por G. O processo de treinamento das GANs continua até que se atinja um equilíbrio entre G e D, indicando que o gerador e o discriminador não estão mais melhorando (Waseem, *et al*., 2023).

O processo de aprendizado das GANs é iterativo, com a rede geradora constantemente aprimorando sua capacidade de criar *deepfake*s convincentes, enquanto a rede discriminadora melhora sua habilidade de detectar falsificações.

> Nos últimos anos, com o avanço do aprendizado profundo (DL) e suas extensões bem-sucedidas na detecção de objetos, rastreamento humano e FER, os pesquisadores começaram a explorar o MER com DL. Embora o MER com DL seja desafiador devido às poucas amostras de MEs e à baixa intensidade, grandes progressos foram feitos no MER por meio do desenvolvimento de redes eficazes, exploração de Redes Adversárias Generativas (GAN) e outras técnicas. Atualmente, o MER baseado em DL atingiu o estado da arte em termos de desempenho (Li, *et al*., 2022).

Outro método que pode ser utilizado para a criação das *deepfake*s é baseado no chamados *autoencoders*, que são redes neurais que aprendem a codificar e decodificar informações visuais, o que pode ser utilizado para manipular as características de uma imagem ou vídeo.

> A rede *deepfake* de *autoencoder* de troca de faces utiliza um codificador compartilhado e dois decodificadores, enquanto o codificador e os dois decodificadores compartilham parâmetros durante o processo de treinamento. Um codificador compartilhado aprende a codificar as não-identidades (vetores latentes) subjacentes tanto ao indivíduo de origem quanto ao alvo. Dois decodificadores reconstroem as faces de origem e alvo a partir de suas respectivas representações de vetor latente. A troca de faces é realizada ao decodificar o vetor latente da face de origem por meio do decodificador de face alvo (Waseem, *et al*., 2023).

Com a evolução das *deepfakes*, sistemas de segurança baseados em biometria facial implementaram medidas adicionais, como a solicitação de ações dinâmicas não planejadas, como piscar ou mover o rosto, para mitigar riscos. Embora essas estratégias aumentem a segurança, também geram fricção na experiência do usuário, exigindo passos extras no processo de autenticação. Essas medidas podem não ser eficazes à medida que as *deepfakes* ficam mais sofisticadas. O setor bancário, em particular, tem grande preocupação com esses riscos, já que as *deepfakes* podem ser usadas para fraudar sistemas de autenticação facial.

2.4 Comparação Entre Microexpressões e Expressões Faciais Comuns

As medidas adicionais descritas no item anterior são baseadas no movimento do rosto e nas expressões faciais do indivíduo que está buscando a autenticação. Por serem expressões e movimentos espontâneos, mesmo que com alta complexidade, as expressões faciais e os movimentos do rosto podem ser simulados pela evolução das GANs. Uma evolução pode ser o uso das microexpressões faciais.

O estudo das microexpressões data da década de 1960 com o objetivo de se avaliar pacientes psiquiátricos quanto a veracidade de suas reações. Esse primeiro campo, que sempre despertou muito interesse da ciência, interfere diretamente com as relações sociais. A descoberta de método científico que possa asseverar a veracidade de uma afirmação feita por outra pessoa é desafio até hoje.

> O fenômeno das MEs foi descoberto pela primeira vez por Haggard e Isaacs em 1966. Três anos depois, Ekman e Friesen também declararam a descoberta de MEs durante a análise de vídeos de pacientes psiquiátricos para a detecção de mentiras. Nos anos seguintes, Ekman e seus colegas continuaram as pesquisas sobre MEs e desenvolveram o Sistema de Codificação de Ação Facial (FACS) e a Ferramenta de Treinamento de Micro-expressões (METT) (Li, *et al*., 2022).

As microexpressões faciais são expressões extremamente breves e involuntárias que revelam emoções verdadeiras, muitas vezes ocultas, e que surgem de forma espontânea em uma fração de segundo.

> Expressão facial (FE) é um dos meios mais poderosos e universais de comunicação humana, estando altamente associada aos estados mentais, atitudes e intenções das pessoas. Além das expressões faciais comuns (também conhecidas como macroexpressões), que observamos no dia a dia, as emoções também podem ser expressas em um formato especial de microexpressões (MEs) em determinadas condições. As MEs são expressões faciais que revelam os sentimentos ocultos das pessoas em situações de alta pressão, quando elas tentam esconder suas verdadeiras emoções. Diferentemente das macroexpressões, as MEs são movimentos faciais espontâneos, sutis e rápidos (de 1/25 a 1/3 de segundo) que reagem a estímulos emocionais (Li, *et al*., 2022).

Microexpressões faciais diferem das expressões faciais principalmente quanto à espontaneidade. São involuntárias, ou seja, não podem ser controladas pelo indivíduo. Outras diferenças importantes também são os tempos de duração e a viabilidade ou não do movimento ser notado sem o uso de recursos tecnológicos.

Um exemplo, uma pessoa sorrindo voluntariamente pode disfarçar seu descontentamento em uma determinada situação. Esse controle consciente das expressões faciais permite que as pessoas manipulem suas interações sociais e

ocultem suas verdadeiras emoções, o que dificulta a detecção de mentiras ou enganações.

Existem duas vias neurais distintas para transmitir o comportamento facial: as vias neurais piramidais e extrapiramidais. A primeira é responsável pelas macroexpressões com ações faciais voluntárias, enquanto a segunda é responsável pelas expressões faciais espontâneas. Em cenários de alto risco, como quando alguém está mentindo, ambas as vias são ativadas e entram em um conflito, resultando no vazamento fugaz de emoções genuínas na forma de microexpressões (Ben, *et al*., 2022).

As expressões faciais simuladas por *deepfake*s, embora convincentes em vídeos mais longos e em situações controladas, muitas vezes falham em replicar a complexidade e a sutileza dos movimentos musculares que ocorrem durante uma microexpressão.

2.5 Sistema de codificação de ação facial (FACS)

Para o tratamento da biometria facial em sistemas computacionais é necessário a definição de padrões codificáveis para que possam ser incorporados aos algoritmos, independente do uso de Inteligência Artificial. Esse padrão foi proposto por Paul Ekman e Wlace Frieses em 1978 (Cohn; Ekman, 2007). Eles desenvolveram o FACS como uma metodologia para categorizar todos os movimentos faciais visíveis, baseando-se na ativação de diferentes músculos faciais, conhecidos como Unidades de Ação (AUs). São 32 Unidades de Ação principais (AUs) que descrevem os movimentos básicos dos músculos faciais.

Essas AUs podem ser combinadas para representar uma ampla variedade de expressões faciais

2.6 Utilização de *deep Learning* para viabilizar o uso de Microexpressões Faciais

Com o objetivo de viabilizar a utilização das microexpressões faciais é necessário recorremos ao uso de tecnologias de Inteligência Artificial, especialmente à *deep learrning*. A DL se propõe a analisar grandes volumes de dados na busca de padrões complexos, características inerentes às ME que possuem a natureza de curta duração e sutileza, exigindo uma análise detalhada e precisa para identificar os sutis

movimentos musculares captados por meio de imagens, analisando-as e identificando esses padrões.

> O reconhecimento de microexpressões pode ser estudado a partir de dois aspectos: detecção de expressões e classificação de expressões. O principal objetivo da primeira é responder se há microexpressões na sequência de imagens, enquanto o último visa determinar a categoria das microexpressões, assumindo que elas estejam presentes na sequência. Além disso, a tarefa de detecção também envolve tarefas avançadas, como determinar o momento de ocorrência (*Onset*), o pico (*Apex*) e o desaparecimento (*Offset*) das microexpressões. Do ponto de vista do aprendizado de máquina, ambas as tarefas são de classificação, de modo que alguns pesquisadores utilizam a mesma lógica para treinar diferentes modelos que solucionem essas duas tarefas (Zhang, 2024).

Outro ponto importante para viabilizar o uso das ME é viabilizar a identificação dos padrões em tempo real, quando o indivíduo está se autenticando. Redes neurais profundas têm a capacidade processar vídeos em tempo real, que é inviável ou mais difícil com técnicas tradicionais de aprendizado de máquina.

Um terceiro fator é a capacidade de abstrair elementos que dificultam a qualidade na coleta das imagens, tais como: iluminação, ângulos e qualidade da câmera, raça e contexto emocional.

Para demonstrar o poder das redes neurais para vencer estes três desafios (vídeos em tempo real, fatores que dificultam a qualidade da imagem e tratamento de volume de dado), trouxemos de (Gotz, 2024) um exemplo do uso de técnicas de Redes Neurais Artificiais para navegação do VANTs (Veículos Aéreos não Tripulados), que exigem processamento de imagens em tempo real para sua navegação, estão sujeitas a todas condições de interferência na captura de imagens e tratam volumes de dados muito acima de uma imagem para reconhecimento facial:

> Nota-se a grande demanda de RNAs como ferramentas que podem ser aplicadas em navegação aérea autônoma de VANTs por imagens, ou pelo menos de estudos comparativos entre estas ferramentas e os algoritmos clássicos de processamento de imagens, visão computacional e reconhecimento de padrões em imagens para a aplicação em questão. Isto porque a navegação aérea autônoma de VANTs exige baixo custo computacional, processamento em tempo real e embarcado, implementação em hardware, tolerância a falhas, entre outros requisitos, que são implementáveis em RNAs (Gotz, 2024).

Destaca-se as técnicas de GAN (Redes Adversárias Generativas) para este propósito de treinamento e teste tendo em vista o objetivo da GAN para gerar novos dados e desafios, apresentando a cada iteração maior acurácia ao sistema.

> Nos últimos anos, com o avanço do aprendizado profundo (DL) e suas extensões bem-sucedidas na detecção de objetos, rastreamento humano e FER, os pesquisadores começaram a explorar o MER com DL. Embora o MER

> com DL seja desafiador devido às poucas amostras de MEs e à baixa intensidade, grandes progressos foram feitos no MER por meio do desenvolvimento de redes eficazes, exploração de Redes Adversárias Generativas (GAN) e outras técnicas. Atualmente, o MER baseado em DL atingiu o estado da arte em termos de desempenho (Li, *et al*., 2022).

Diante disso, é essencial para que possa ser viabilizado o uso de microexpressões faciais, para fins de segurança, a associação com *deep learrning*.

Alguns estudos focados em expressões faciais foram analisados para avaliar outras técnicas. Em (Agarwal, *et al*., 2023) encontramos uma abordagem denominada multimodal semântica que utiliza múltiplas formas de análise visual e semântica para identificar *deepfakes*. Esta técnica avalia os movimentos faciais e as palavras do vídeo. Utiliza também as AU's e se propõe a identificar padrões biométricos de forma única.

Em (Naghavi, *et al,* 2021) é apresentado um método que explora as características espaço-temporais para detecção e localização de *deepfakes*. das microexpressões faciais ao longo de vários quadros do vídeo para buscar exatamente onde houve a manipulação. Neste caso, o desafio é quanto à qualidade da amostra.

Em (Mitra *et al*., 2021), foi proposta uma abordagem de aprendizado de máquina para detectar *deepfakes* em vídeos comprimidos de redes sociais, utilizando uma ombinação de redes neurais convolucionais (CNN) e um classificador. A técnica se baseia na extração de quadros-chave, reduzindo a complexidade computacional. É mais eficaz em vídeos que utilizam autoencoders ou redes adversárias generativas (GANs), e se aplica particularmente bem a *deepfakes* que envolvem manipulação facial, identificando artefatos visuais como diferenças na cor da pele e imprecisões nos detalhes faciais.

Embora os estudos apresentem técnicas inovadoras e promissoras, não vemos aplicabilidade delas para o problema enfrentado neste ensaio teórico, pois a limitação da primeira em relação ao grande volume de dados para treinamento da IA e para o segundo, a alta qualidade na coleta do vídeo e o grande número de quadros para a comparação das alterações, tornam inviáveis para a autenticação do cliente em tempo real. No caso do terceiro estudo, ele não foca microexpressão e sim a expressão facial tradicional. Traz uma contribuição importante ao utilizar vídeo comprimido, que é a qualidade similar a dos vídeos a serem analisados pela proposta deste ensaio.

3 CONSIDERAÇÕES FINAIS

O setor bancário tem a confiança como principal pilar. O ato de depositar bens e direitos em uma instituição é acima de tudo a demonstração de confiança naquela instituição e no Sistema Financeiro que a regula e fiscaliza.

Consolidar uma imagem de solidez e responsabilidade é um esforço contínuo para as instituições financeiras. Fator decisivo para manter essa confiança e a garantia de integridade e segurança aos clientes.

O resultado no nível estratégico da ação de usar inteligência artificial e microexpressões faciais para mitigar os riscos de *deepfakes* na autenticação biométrica facial no setor financeiro pode ser analisado em várias dimensões:

a. Aumento da Segurança: A capacidade de identificar *deepfakes* em tempo real aumenta a proteção contra fraudes, resultando em menos perdas financeiras e aumentando a confiança nas transações digitais.
b. Fortalecimento da Confiança do Consumido: Os clientes tendem a confiar mais nas instituições financeiras que implementam tecnologias avançadas de segurança, o que pode resultar em maior adesão a serviços digitais.
c. Vantagem Competitiva: Instituições que adotam essas tecnologias podem se destacar no mercado, atraindo clientes que valorizam segurança e inovação.
d. Compliance e Regulamentação: A implementação de medidas robustas de segurança ajuda as instituições a atenderem regulamentos e normas de segurança cibernética, evitando penalizações.
e. Eficiência Operacional: A automação da verificação de identidade com IA pode reduzir o tempo necessário para autenticação, melhorando a experiência do usuário e a eficiência operacional.
f. Inovação Contínua: O investimento em tecnologias avançadas promove uma cultura de inovação dentro da organização, incentivando mais pesquisas e desenvolvimento em segurança cibernética.
g. Uso natural pelos clientes: Quando se trata de segurança de grande número de pessoas, e em bancos que podem possuir centenas de milhões de clientes, o sistema de segurança tem que ser intuitivo e de uso comum para o cliente.
h. Viabilidade Financeira: Mais um ponto positivo para a biometria facial, pois o dispositivo, predominante, de captura usado hoje, o celular, é de uso cotidiano dos clientes, não havendo necessidade de investimentos. Por fim, sendo o

equipamento de propriedade do cliente, torna o seu uso mais confiável também.

Esses resultados no nível estratégico não apenas fortalecem a posição das instituições financeiras em um mercado competitivo como também contribuem para a estabilidade e segurança do sistema financeiro.

Com o crescimento exponencial das *deepfake* manipulando imagens, características acústicas da voz e vídeo cresce a preocupação com nível de confiança da biometria facial para soluções críticas. Soluções como requisitar ao cliente que faça movimentos não planejados, dificultam o uso de *deepfake* em tempo real, porém geram fricção com o cliente, o que pode inibir o uso da tecnologia, induzindo o cliente a ativar outros meios de acessos de menor segurança, como o retorno ao uso de usuário e senha.

A busca por referência para este ensaio teórico, especificamente quanto ao tema das microexpressões faciais, foi árdua por conta do baixo número de publicações relacionadas ao tema nos repositórios nacionais. Nos repositórios externos conseguimos encontrar maior número de bibliografia, em geral a partir de 2021, reforçando o exposto no texto, de que a tecnologia de microexpressões faciais está em desenvolvimento, tendo desafios a serem superados para ampla utilização, destacando-se:

a. Equipamento de coleta: Em geral são celulares, que apresentam amplo espectro de mercado, o que pode restringir ou gerar nicho em um primeiro momento. Atualmente, poucos dispositivos possuem tecnologia avançada o suficiente para atender às exigências de captura de microexpressões para detecção de *deepfakes.* No contexto bancário, as instituições financeiras são obrigadas a informar ao Banco Central movimentações superiores a R$ 30 mil, conforme estabelece a Instrução Normativa da Receita Federal nº 1.761/2017. A utilização da tecnologia de detecção de *deepfake*, em um estágio inicial de utilização, poderá fortalecer a legitimidade dessas transações, oferecendo uma camada adicional de segurança.
b. A qualidade da coleta da imagem, sensível à iluminação e à posição. Serão necessários cuidados adicionais para uma correta captura, além de um intenso treinamento das redes neurais para reconhecimento das microexpressões nas imagens capturadas.

Se por um lado temos esses desafios a vencer, por outro lado, o potencial de uso da tecnologia é muito mais amplo, além do setor bancário. O uso de *deepfake* vai desde a distribuição de informações falsas sem fins maliciosos até a interferência nas eleições de um país, expressão maior da soberania de um povo. Também, inclui-se neste conjunto de potenciais usos todos aqueles que utilizam certificações por meio de vídeo chamadas, como a prova de vida da Previdência Social ou o padrão Ouro do e-GOV.

Uma tecnologia confiável e sem eventuais contestações jurídicas, com redução de viés de raça e cor (microexpressão pode ser menos sensível a questões de raça), pode ser aplicada no campo da Segurança Pública e de Estado.

Reforça também a redução desses viéses o fato do modelo ser treinado com a população brasileira em função da sua grande miscigenação. Incorporando a base do país importador da tecnologia, teríamos um amplo espectro racial para redução do víeis.

O uso da solução não se restringe ao setor financeiro, é possível utilizá-la por exemplo, nos embarques e desembarques de aeroportos e portos buscando pessoas com alguma pendência judicial e para a identificação de pessoas em eventos públicos.

Concluindo, considero que o estudo demonstrou a importância da biometria facial como estratégia confiável para identificação pessoal. Demonstrou também que o uso das microexpressões faciais, aliado ao processamento com redes neurais profundas, pode ser um fator mitigador dos riscos que as *deepfake*s representam para burlar os sistemas baseados nessa tecnologia.

No campo da segurança cibernética, demonstrou o potencial da tecnologia para o setor financeiro. No campo da defesa, demostrou ser uma solução para auxiliar a proteção das infraestruturas críticas, aliado ao combate ao terrorismo com a proteção de fronteira e ao ciberataques à soberania nacional que utilizam *deepfake*, como já está ocorrendo nas campanhas eleitorais.

Com esses atores temos dois fortes aliados com interesses convergentes para compor a tríplice hélice de inovação, criando condições para uma importante tecnologia de segurança de propriedade nacional.

REFERÊNCIAS

AGARWAL, Shruti; HU, Liwen; NG, Evonne; DARRELL, Trevor; LI, Hao; ROHRBACH, Anna. **Watch Those Words: Video Falsification Detection Using Word-Conditioned Facial Motion**. *In:* INTERNATIONAL CONFERENCE ON COMPUTER VISION. BERKELEY. New York: IEEE, 2023.

AKAMAI. **Navigating the rising tide**: attack trends in financial services. Cambridge, MA: AKAMAI, 2024. Disponível em: https://www.akamai.com/resources/state-of-the-internet/financial-services-trends-2024. Acesso em: 16 set. 2024

BANCO CENTRAL DO BRASIL. **Resolução CMN nº 4893, de 26 de fevereiro de 2021**. Estabelece critérios para a classificação de ativos financeiros no âmbito do sistema financeiro nacional. Brasília, DF: BC, 2021. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo/numero=4893. Acesso em: 16 set. 2024.

BEN, Xianye; REN, Yi; ZHANG, Junping; WANG, Su-Jing; KPALMA, Kidiyo; MENG, Weixiao; LIU, Yong-Jin. **Video-based facial micro-expression analysis**: a survey of datasets,features and algorithms. New York: IEEE, 2021. Disponível em: https://ieeexplore.ieee.org/document/9382112. Acesso em: 16 set. 2024.

BLACKBURN, David M.; BONE, John M.; WENTWORTH, Bruce L. **Biometrics: history, challenges, and opportunities.** MITRE Corporation, 2006. Technical Report. Disponível em http://www.biometricscatalog.org/NSTCSubcommittee. Acesso em: 16 set. 2024.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 16 set. 2024.

BRASIL. **Receita Federal. Instrução Normativa RFB nº 1761**, de 20 de novembro de 2017. Dispõe sobre a prestação de informações para fins de consolidação de débitos previdenciários no âmbito do Programa de Regularização Tributária (PRT) de que trata a Medida Provisória nº 783, de 31 de maio de 2017. Diário Oficial da União: Seção 1, Brasília, DF, p. 45, 21 nov. 2017.

CARVALHO, Fernando Cardim de. **Risco sistêmico, fragilidade financeira e crise**: uma análise pós-keynesiana a partir da contribuição de Fernando Cardim de Carvalho. Revista de Economia Contemporânea, [*S. l.*], v. 24, n. 1. 2020. Disponível em: https://www.scielo.br/j/rec/a/JgzfgVynVnd9RgjL8VBTjXJ/?lang=pt. Acesso em: 20 set. 2024.

COHN, J. F.; AMBADAR, Z.; EKMAN, P. **Observer-based measurement of facial expression with the Facial Action Coding System**. *In*: COAN, J. A.; ALLEN, J. J. B. (ed.), Handbook of emotion elicitation and assessment. Oxford: Oxford University Press, 2007. p. 203–221

DINIZ, Fábio Abrantes. **RedFace**: um sistema de reconhecimento de expressões faciais para apoiar um ambiente virtual de aprendizagem. 2013. Dissertação (Mestrado em Ciência da Computação) – Universidade Federal Rural do Semi-Árido; Universidade do Estado do Rio Grande do Norte, RN, 2013. Disponível em: semanticscholar.org. Acesso em: 16 set. 2024.

ESCOLA SUPERIOR DE GUERRA (Brasil). Site: **Escola Superior de Guerra – ESG**. Disponível em: https:// https://www.gov.br/esg/pt-br/a-esg. Rio de Janeiro: ESG, 2023. Acesso em: 20 set. 2024.

ETZKOWITZ, Henry. **Hélice Tríplice**: inovação e empreendedorismo universidade-indústria-governo. Estudos Avançados, São Paulo, v. 24, n. 66, p. 293-315, 2017. Disponível em: https://www.scielo.br/j/ea/a/4gMzWdcjVXCMp5XyNbGYDMQ/?lang=pt. Acesso em: 20 set. 2024.

FANAYA, Aline Vanessa Caetano. **Fake news e tecnologias de manipulação de mídia**: o potencial perigoso dos d*eepfake*s na era digital. São Paulo: Editora X, 2021. Disponível em: https://revistas.pucsp.br/index.php/teccogs/article/view/55982/37930. Acesso em: 16 set. 2024.

FEDERAÇÃO BRASILEIRA DE BANCOS (FEBRABAN). **Pesquisa Febraban de Tecnologia Bancária 2024**: transações. São Paulo: FEBRABAN, 2024. Disponível em: https://portal.febraban.org.br/pagina/3106/48/pt-br/pesquisa. Acesso em: 16 set. 2024.

FEITOSA, Conceição de Maria Graça Barros. **Transformação digital**: o impacto das fintechs na performance financeira do mercado bancário brasileiro. 2020. Dissertação (Mestrado em Economia) – Instituto Brasiliense de Direito Público, Brasília, DF, 2020.

FÓRUM ECONÔMICO MUNDIAL. **Fostering effective energy transition**: insight report. Geneve: FEM, 2024. Disponível em: https://www.weforum.org. Acesso em: 23 set. 2024.

FUNDO MONETÁRIO INTERNACIONAL(FMI). **Global financial stability report**: the last mile: financial vulnerabilities and risks. Washington, DC: IMF, 2024. Disponível em: *https://www.imf.org/en/Publications/GFSR*. Acesso em: 23 set. 2024.

GOTZ, Gustavo Augusto Mascarenhas. **Redes Neurais Artificiais em Imagens para Estimação da Posição de um VANT**. 2024. Dissertação (Mestrado em Computação Aplicada) – Instituto Nacional de Pesquisas Espaciais (INPE), São José dos Campos, 2024. Disponível em: http://dspace.sti.ufcg.edu.br:8080/jspui/handle/riufcg/29315. Acesso em: 19 set. 2024.

KRISHNAN, Armin; KASSA, Hanna Sammir. **O crepúsculo da hegemonia do dólar americano e o mundo multipolar que se aproxima**. Austral: Revista Brasileira de Estratégia e Relações Internacionais, v. 12, n. 24, p. 36-52, jul./dez. 2023. Disponível em: https://seer.ufrgs.br/index.php/austral/article/view/130226/91592. Acesso em: 23 set. 2024.

KRUCHIN, Rafael. **Lula's quest for a diplomatic balance Amid Israel-Hamas war**. Americas Quarterly, 18 Oct. 2023. Disponível em: https://www.americasquarterly.org/article/lulas-quest-for-a-diplomatic-balance-amid-israel-hamas-war/. Acesso em: 23 set. 2024.

JAIN, Anil K.; NANDAKUMAR, Karthik; ROSS, Arun. **50 years of biometric research**: Accomplishments, challenges, and opportunities. Journal of Pattern Recognition, 2016. Disponível em: https://www.researchgate.net/publication/290509735. Acesso em: 16 set. 2024.

LI, Yante; WEI, Jinsheng; LIU, Yang; KAUTTONEN, Janne; ZHAO, Guoying. **Deep Learning for Micro-Expression Recognition**: A Survey. IEEE Transactions on Affective Computing, v. 13, n. 4, p. 1-17, Oct./Dec. 2022. Disponível em: https://arxiv.org/abs/2107.02823. Acesso em: 16 set. 2024.

MARCONDES, Danilo; SILVA, Antonio Ruy de Almeida. **The role of Brazil in the Russia-Ukraine conflict**: a potential peace enabler? Journal of International Affairs, v. 75, n. 2, Spring/Summer, 2023. Disponível em: https:// https://jia.sipa.columbia.edu/content/role-brazil-russia-ukraine-conflict-potential-peace-enabler. Acesso em: 23 set. 2024

MAZIERO, Carlos. **Sistemas operacionais: conceitos e mecanismos**. Curitiba : DINF - UFPR, 2019. Cap. 28, p. 371

MITRA, Alakananda; MOHANTY, Saraju P.; CORCORAN, Peter; KOUGIANOS, Elias. **A machine learning based approach for deepfake detection in social media through key video frame extraction**. SN Computer Science, v. 2, n. 98, 2021. DOI: https://doi.org/10.1007/s42979-021-00495-x.

MIRSKY, Yisroel; LEE, Wenke. **The Creation and detection of deepfakes**: a survey. Georgia: Georgia Institute of Technology; Ben-Gurion University, 2016. Disponível em: https://arxiv.org/pdf/2004.11138. Acesso em: 16 set. 2024.

NAGHAVI, Meysam; ZHANG, Jiachun; GAN, Chuang; POGGIO, Tomaso. **Exploring Spatial-Temporal Features for Deepfake Detection and Localization**. *In*: INTERNATIONAL CONFERENCE ON COMPUTER VISION (ICCV), 2021. New York: IEEE, 2021. Disponível em: https://arxiv.org/abs/2210.15872 . Acesso em: 4 out. 2024.

ROUSAN, Mohammad Al; INTRIGILA, Benedetto. **A Comparative analysis of biometrics types**: literature review. Journal of Computer Science, Rome, 2020. Disponível em: https://www.researchgate.net/publication/347971656_A_Comparative_Analysis_of_Biometrics_Types_Literature_Review. Acesso em: 16 set. 2024.

SOUZA, Marco Antônio de. **A Biometria e suas Aplicações**. Revista Brasileira de Ciências Policiais, Brasília, DF, v. 11, n. 2, p. 79-102, maio/ago. 2020. Disponível em: https://periodicos.pf.gov.br/index.php/RBCP/article/view/710. Acesso em: 16 set. 2024.

ZHANG, Yifei. **A Review of deep learning-based micro-expression classification**. Beijing: Institute of Technology, 2024. Disponível em: https://drpress.org/ojs/index.php/HSET/article/view/21655. Acesso em: 19 set. 2024

WASEEM, Saima; ABU BAKAR, Syed Abdul Rahman Syed; AHMED, Bilal Ashfaq; OMAR, Zaid; EISA, Taiseer Abdalla Elfadil; DALAM, Mhassen Elnour Elneel. **Deepfake on face and expression swap**: a review. New York: IEEE, 2023. Disponível em: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10285057. Acesso em: 16 set. 2024.