Interference Journal
ISSN 2009-3578
DOI
A2 QUALIS SUCUPIRA
2017-2020

A IDENTIFICAÇÃO HUMANA: MECANISMO PREVENTIVO DE CONTENÇÃO DE AMEAÇA DIGITAL NO ESPAÇO CIBERNÉTICO.

Rair Silva e Souza de Moura[1], Nélio António Covane [2], Hewerson Silva Figueira[3], Cesar Mauricio de Abreu Mello[4] e Raylene Rodrigues de Sena[5]

https://doi.org/10.36557/2009-3578.2025v11n2p6260-6283
Artigo recebido em 30 de Agosto e publicado em 30 de Outubro de 2025

ARTIGO ORIGINAL

RESUMO:

O avanço das tecnologias digitais alterou radicalmente a forma como os indivíduos se constituem enquanto sujeitos sociais, tornando a identidade humana uma construção híbrida entre o físico e o digital. **A introdução:** a identidade digital emerge como representação algorítmica da identidade humana, composta por dados e metadados coletados em ambientes online. **Objetivo:** rever as discussões sobre a identificação humana segundos alguns teóricos Castells (2003), Zuboff (2018), Gates (2005) e Hadnagy (2018), com a finalidade de entender os *insights* da identificação humana na a transição para o ciberespaço, considerando os riscos, controle algorítmico, manipulação

[1]Administradora, Pós-Graduada em Segurança Pública, Cidadania e Direitos Humanos pela Faculdade Metropolitana do Amazonas- FAMETRO, Pós-graduanda em Direito Público e Mestranda em Segurança Pública, Cidadania e Direitos Humanos pela Universidade do Estado do Amazonas- PPGSP/UEA. Servidora da Polícia Civil do Amazonas- PC/SSP/AM. Email: rair_moura@hotmail.com, **lattes:** 7078548523224836 e **orcid**: 0009-0000-4845-4907.
[2]Mestrando no Programa de Pós-Graduação em Segurança Pública, Cidadania e Direitos Humanos (PPGSP) pela Universidade Estadual de Amazonas (ESO-UEA). Licenciado em Relações Internacionais e Diplomacia, pelo Instituto Superior de Relações Internacionais (ISRI, Moçambique). E-mail: nelcovane@gmail.com, **lattes:** 9053071120074627 e **orcid**: 0009-0002-3689-8396.
[3] Administrador, Pós-Graduado em Segurança Pública e Direitos Humanos pela Faculdade Metropolitana do Amazonas – FAMETRO, Mestrando em Segurança Pública, Cidadania e Direitos Humanos pela Universidade do Estado do Amazonas-PPGSP/UEA. Servidor da Polícia Civil do Amazonas- PC/SSP/AM. E-mail:hewersonfigueira6@gmail.com, **lattes:** 2710456242551123 e **orcid**: 0009-0003-6655-4065.
[4] Doutor em Desenvolvimento Sustentável do Trópico Úmido, docente do Programa de Pós-graduação em Segurança Pública da UFPA. E-mail: mello.cesar@gmail.com, **lattes:** 2079368341132335 e **orcid**: 0000-0003-3086-2624.
[5] Raylene Rodrigues de Sena Doutora em Administração Universidade Federal de Minas Gerais (UFMG). Manaus, Amazonas, Brasil. rsena@uea.edu.br, **lattes:** /0000-0001-5263-6981 e **orcid**: 6625850476389896.

psicológica e aspectos ético-jurídicos. A **metodologia** é qualitativa, com análise crítica e interdisciplinar. Em **Conclusão**, o trabalho propõe diretrizes de governança, proteção e cidadania digital frente à complexidade das identidades mediadas por tecnologia.

PALAVRAS-CHAVE: Identidade digital. Ciberespaço. Segurança da informação. Engenharia social. Governança de dados. Cidadania digital.

THE HUMAN IDENTIFICATION: A PREVENTIVE MECHANISM FOR CONTAINING DIGITAL THREATS IN CYBERSPACE.

ABSTRACT

The advancement of digital technologies has radically altered the way individuals constitute themselves as social subjects, making human identity a hybrid construction between the physical and the digital. Introduction: Digital identity emerges as an algorithmic representation of human identity, composed of data and metadata collected in online environments. Objective: To review discussions on human identification according to theorists Castells (2003), Zuboff (2018), Gates (2005), and Hadnagy (2018), with the aim of understanding the insights of human identification in the transition to cyberspace, considering risks, algorithmic control, psychological manipulation, and ethical and legal aspects. The methodology is qualitative, with critical and interdisciplinary analysis. Thus, in Conclusion, the work proposes guidelines for governance, protection, and digital citizenship in light of the complexity of technology-mediated identities.

KEYWORDS: *Digital Identity. Cyberspace. Information Security. Social Engineering. Data Governance. Digital Citizenship.*

Instituição afiliada – Universidade Estadual de Amazonas (ESO-UEA).

INTRODUÇÃO

A identidade humana tem sido profundamente impactada pela revolução digital das últimas décadas, afastando-se, dos paradigmas ortodoxos e bases estruturais das nossas sociedades. Estas que foram construídas em séculos com determinantes estruturada físicos, sociais e culturais. Assim, com os esforços de consolidação das Tecnologias da Informação e Comunicação (TICs), o sujeito contemporâneo passou a existir simultaneamente em duas esferas: a presencial e a virtual. Sendo a última, um novo cenário que implica as interações digitais que por sua vez implicam em trocas de dados. Ainda que, regularmente, de forma inconsciente, os mesmos dados passem a constituir uma nova dimensão da identidade: a identidade humana digital.

Esta nova identidade humana passa a ser caraterizada e dimensionada por padrões de acessos digitais, registros biométricos, históricos de navegação, geolocalizações e interações em redes sociais. Fatores que determinam a nova interação dos atores virtuais, cuja mudança interativa não é apenas técnica, mas também política, jurídica e ética, implicam na redefinição da privacidade, autonomia e noção de subjetividade.

Segundo Castells (2003), vivemos na era da sociedade em rede, na qual a informação e os fluxos digitais tornam-se os principais organizadores da vida social e econômica. A identidade deixa de ser construída apenas por meio da convivência social direta e passa a ser mediada por algoritmos, dispositivos e bancos de dados, alterando as estruturas tradicionais de reconhecimento, pertencimento e controle.

Esse novo contexto requer uma análise interdisciplinar que contemple as implicações da transição da identidade humana para o ciberespaço. Este artigo se propõe a realizar essa análise, com foco em três eixos principais: a constituição da identidade digital, os riscos associados à sua exposição e manipulação, e as estratégias de governança e proteção frente à crescente complexidade do ambiente digital.

METODOLOGIA

Metodologia pode ser entendida comom o conjunto de etapas que orientam ao pesquisador a formulação do problema para análise dos resultados concernenetes ao mesmo e, segundo Gil (2010, p. 26-29) podem ser destacadas as pesquisas exploratórias, descritivas e explicativa. E neste artigo foi adotada a pesquisa descritiva de caracter qualitativa, entendendo-se por qualitativa a pesquisa que, segundo Minayo (2014, p. 21) busca compreender significados, interpretações e contextos sociais, indo além de números e frequências. Fundamentos que permitiram entender os contornos de analises sobre a identificação humana em uma perspectiva crítica e interdisciplinar.

RESULTADOS E DISCUSSÃO

2.1 IDENTIDADE HUMANA E IDENTIDADE DIGITAL: CONCEITUAÇÃO E EVOLUÇÃO

A. Identidade Humana na Tradição Sociocultural

A identidade humana pode ser compreendida como um conjunto de atributos pessoais, sociais, psicológicos e culturais que definem o sujeito em sua singularidade e pertencimento coletivo. Ela é moldada pelas experiências de vida, pela história familiar, pelo contexto sociocultural e pelas interações interpessoais. E para Castells (2003), a identidade na sociedade contemporânea, é o fruto de uma construção resultante de processos de legitimação (identidade institucional), resistência (identidade de oposição) e projeto (criação de novas formas indenitárias). Fatores que estruturariam esta construção que, se entende ser, dinâmica e constantemente sujeita às reconfigurações sociais conforme os contextos históricos e tecnológicos.

As sociedades contemporâneas, hoje, também estão imersas numa realidade virtual que estrutura a necessidade de identidade humana digital para engajamento e

interação virtual, fenômeno consequente do advento da era digital e, com ela, uma nova camada indenitária (a identidade digital). Uma identidade que, Jain, Dass e Nandakumar (2004), bem como Fernandez (2023) entendem ser um processo de procura e comparação de amostra biométrica em base de dados para encontrar o registro associado a um único indivíduo (um-para-muitos)[6]. Uma abordagem que expõe o entendimento amplo de identificação que estabelece através de antecedentes necessários para o entendimento da identidade através do elemento verificação.

A esta realidade, Neurotech (2024) define a identidade digital como a representação de uma entidade (pessoa, máquina, aplicação, objeto físico ou empresa) num contexto digital. E Gates (2005) subscreve esta ideia descrevendo que a identidade digital é composta por informações que representam os indivíduos em ambientes virtuais — nome de usuário, senhas, dados biométricos, e-mails, registros de localização e preferências de navegação. E esses dados são capturados durante interações com dispositivos, plataformas e serviços online, sendo muitas vezes armazenados indefinidamente por terceiros.

Ao exposto, a identidade digital passa a ser o reflexo da identidade humana e um produto algorítmico, ainda que, resulte no que se refere como capitalismo de vigilância[7], este que crie representações que não são controladas nem acessadas integralmente pelos próprios titulares (Zuboff, 2018). E a identidade digital, deixa assim, de ser uma expressão autônoma do sujeito e passa também, a ser uma ferramenta de previsão e manipulação. ainda que, para Santos (2023), a gestão de identidade e o respectivo acesso[8] passam a ser muito mais relevantes para a segurança de identidades. E no Brasil, por exemplo, segundo o Portal Gov.br (2023), o governo brasileiro expõe uma solução digital para validação de identidade através do Datavalid

[6] Este processo se compõe no preceito da verificação ou autenticação que, é o processo de confirmar se uma amostra biométrica corresponde a uma amostra de referência específica já existente no sistema (um-para-um) (Jain; Dass; Nandakumar, 2004; Fernandez, 2023).
[7] Para Zubof (2018), o" capitalismo de vigilância", se entende como uma experiência humana convertida em dados comportamentais com valor de mercado. A exploração e processamento de dados pessoais dos usuários com base em interesses comerciais ou operacionais.
[8] Um conjunto de processos, políticas e tecnologias que garantem a identidade de uma entidade, a qualidade de suas informações, além de autenticação, autorização, responsabilização e auditoria em ambientes online (ESR, n.d.).

que faz a qualificação cadastral de pessoas e instituições mediante consultas em bases governamentais.

Porém, a multiplicidade de perfis online também fragmenta a noção tradicional de identidade (Zuboff, 2018). Isso constata-se em realidades que, por exemplo, o mesmo sujeito pode apresentar versões distintas de si em diferentes plataformas: profissional no LinkedIn, pessoal no Instagram, opinativo no X (antigo Twitter), lúdico no TikTok, etc. Situações estas que, exige algum rigor acrescido em análises sobre as construções distintas da identidade, o que pode gerar conflitos entre a autoimagem e a percepção pública. Contudo, nessa fragmentação, como o autor enfatiza, ainda que se permita liberdade de expressão, o usuário também se expõe à riscos, como a vigilância cruzada, julgamento social, sobrecarga emocional e perda da coesão identitária.

2.2. PSICODINÂMICA DA IDENTIDADE NO AMBIENTE DIGITAL

O comportamento humano pode ser um elemento analítico fundamental em análises sobre a identidade e a segurança. E o ambiente digital emerge como um dos determinantes da questão comportamental na análise, considerando que, esta, pode influenciar na maneira de identificação pessoal e o padrão comportamental indenitário adaptado no contexto virtual (o sujeito pode atuar sob diferentes identidades). Gerando uma fluidez identitária pode reduzir o senso de responsabilidade ou de realidade, facilitando comportamentos que periguem a outros usuários.

Esta realidade supracitada para Zuboff (2018, p. 264), gera o fenômeno da “desindividualização algorítmica”, em que o indivíduo deixa de se perceber como sujeito e passa a agir como dado ou estatística. O que, consequentemente, se absorve em alienação identitária ou se cria um distanciamento entre o “eu físico” e o “eu digital”, gerando ainda exposições excessivas a vulnerabilidade de ameaças digitais, onde o sujeito tem baixa proteção de dados e vive em negligência às práticas seguras de coexistência virtual.

A. Rastros Digitais e Identidade Preditiva

A exposição de dado digitais, ainda que em ato de socialização, permite a identificação dos respectivos usuários no mundo virtual. E a cada ação neste ambiente, estes servem de rastros deixados pelos mesmos usuários, que são partes que compõem sua identidade (digital). Esses rastros incluem não apenas os dados fornecidos conscientemente, mas também os metadados — como localização, tipo de dispositivo, tempo de permanência em páginas, velocidade de digitação e até o padrão de toque na tela. Essas informações são processadas por algoritmos que constroem modelos preditivos de comportamento. "Excedente comportamental" que, Zuboff (2018) também o classifica como dados coletados além do necessário para o serviço, com o objetivo de previsão e manipulação. Assim, os rastros passam a ser parte de identidade preditiva dos usuários.

Destacamos, à guisa de exemplo, um dos casos mais emblemáticos da exploração indevida da identidade digital que resultou em um escândalo na Cambridge Analytica. Um professor de psicologia coletou e usou dados de milhões de usuários do Facebook para construir perfis psicológicos e direcionar propaganda política personalizada. Nesta realidade, conforme reportado por Zuboff (2018, p. 332), a empresa usava perfis de personalidade baseados no modelo OCEAN (Abertura, Consciência, Extroversão, Amabilidade e Neuroticismo) para adaptar o conteúdo às emoções e preferências do usuário. A manipulação não era explícita, mas emocional e comportamental, atingindo o cerne da autonomia individual.

B. Comportamentos de Alto Risco

Segundo o relatório do *National Cyber Security Centre* (NCSC, 2022), os principais comportamentos de risco incluem: uso de senhas fracas ("123456"), reutilização de senhas (mesma senha para múltiplos serviços), exposição em redes sociais (fotos com localização, documentos pessoais, hábitos de rotina), clique em links encurtados e não verificados, e compartilhamento de dados pessoais em jogos e *quizzes o*nline. Esses comportamentos facilitam ataques de *spear phishing*, sequestro de conta (*account hijacking*) e fraudes de identidade.

Neste contexto, a realidade exposta da identidade digital também passa a ser alvo de diversos crimes, tais como: furto de identidade (*identity theft*), estelionato digital (fraude bancária, boletos falsos), falsidade ideológica em ambiente eletrônico, violação de dispositivos e sistemas, distribuição de *deepfakes* ou uso indevido de imagem. E estes crimes relacionados à identidade digital são infrações que exigem atualizações constantes no ordenamento jurídico, além de cooperação internacional entre as polícias, promotores e empresas de tecnologia para a segurança preventiva e dissipação das ameaças.

2.3. MECANISMOS DE IDENTIFICAÇÃO HUMANA: FERRAMENTAS DE PREVENÇÃO

A. Autenticação e Segurança da Identidade no Ciberespaço

A segurança da informação é sustentada pela Confidencialidade, Integridade e Disponibilidade (os pilares da tríade CIA). Sendo a autenticação o primeiro e fundamental passo para garantir o acesso à sistemas, dados ou plataformas para indivíduos autorizados em determinada instituição. E, por assim ser, o primeiro nível de segurança de informação que merece maior abrangência analítica no artigo.

Uma análise retrospectiva sobre a (in)segurança virtual permite aferir a tipificação da identidade biológica e comportamental[9] e, a identidade digital, como entidade natural ou jurídica com representação no ambiente online. E, em ambas as tipificações, por exemplo, prevalece os mesmos mecanismos de identificação e autenticação (senhas, autenticação multifatores e a biometria). Ainda que, segundo PROTIVITI INC (2024) e Santos (2024) as senhas são o modelo de autenticação mais tradicional.

[9] Segundo Fernandez (2023), o biológico e comportamental baseia-se na premissa de unicidade do indivíduo (ser único) com características físicas e comportamentais distintas, que constituem base de identificação humana digital nos sistemas biométricos de identificação e autenticação.

Neste âmbito, a biometria (do grego "bio"=vida e "metria"=medida) é considerada, segundo Fernandez (2023), o reconhecimento automatizado de indivíduos por meio de suas características comportamentais ou biológicas para medir ou discriminar a identidade de um indivíduo a partir das suas marcas biológicas.

B. O ecossistema da autenticação na Proteção da Identidade

A autenticação é o processo de verificação da identidade de um utilizador ou dispositivo para garantir a sua legitimidade (Santos, 2023). E como destaca Santos, esta é uma etapa crucial para a segurança da informação, pois é através deste processo que os sistemas e dados são protegidos contra acessos não autorizados e ataques cibernéticos. Assim, em resultado da abordagem que se adapte no processo de autenticação, o cidadão pode estar ou não exposto ou vulnerável a determinado nível de ameaça à sua identidade digital. E, como ainda expõe Santos (2023), a autenticação fraca é comparada ao Cavalo de Troia: a qualidade da autenticação (simples ou complexa) pode ser ou não a chave de proteção de seus dados e permitir ou não a efetivação de ataques cibernéticos. Ações que, em função da abordagem adaptada, também podem ou não conceder aos invasores a possibilidade de comprometer a integridade dos dados dos sujeitos de internet.

Para Neurotech (2025), tradicionalmente, a autenticação se baseava em fatores como algo que se sabe (senhas) ou algo que se possui (cartões, smartphones). No entanto, atualmente, a utilização de apenas uma senha já não é suficiente, considerando que, segundo Ecotrust (2020), PROTIVITI INC (2024) e Santos (2023), as senhas, frequentemente são associadas como como elo mais fraco na cibersegurança por serem de fácil roubo, adivinho ou reutilização. Ademais, considerando que, como destaca Neurotech (2025), a tendência atual da autenticação é a combinação de múltiplos fatores de autenticação (MFA), de forma a aumentar a robustez do processo de autenticação e minimizar o risco potencial da efetivação de crimes cibernéticos e fugas de dados caso uma credencial seja comprometida.

Os diferentes tipos de sistemas biométricos oferecem um aumento significativo na acurácia do sistema de comparação, compensando as limitações de fontes

biométricas únicas (Jain, Flynn & Ross, 2007; Ross, Nandakumar & Jain, 2006; Jain, Ross & Nandakumar, 2011a; Fernandez, 2023). E a identificação através da biometria tem resultado ser a abordagem mais adaptada na segurança de informação.

No entendimento de Jain, Dass e Nandakumar (2004), bem com Fernandez (2023), este processo traz uma abordagem cabal no entendimento de identificação que estabelecem antecedentes a percepção da identidade digital através do elemento verificação. Assim todo o processo de acesso e gestão de informação digital se daria depois da identificação digital biométrica do usuário humano, mesmo que sejam entidades jurídicas, como organizações, instituições e outros.

Revisando este processo de autenticação para identificação, se constata que ela se fortalece em características biométricas que incluem traços fisiológicos e comportamentais. Isto é, se por um lado, aos traços físicos da biometria incluem impressões digitais[10], reconhecimento facial[11], Íris, Retina[12] e DNA[13], os traços comportamentais, pertinentes na identificação humana, por outro lado, incluem, segundo Fernandez (2023), a biometria sutil, biometria onipresente e biometrias tradicionais. Ademais, há elementos de identificação humana através da voz e marcha[14], caligrafia (ou escrita)[15] e biometria comportamental[16].

A estas caraterísticas, Duarte (2021) elucida que elas devem possuir unicidade, perenidade, imutabilidade (biológicas), praticabilidade e técnicas de classificação.

---

[10] Segundo Maltoni (2009), Jain, Chen e Demirkus (2007) e Jain, Ross, Nandakumar (2011a), assim como Fernandez (2023) estes traços são formadas por padrões de cristas e sulcos, com suas "minúcias" ou os respetivos pontos característicos (terminações e bifurcações) eternamente.
[11] Jain, Ross e Nandakumar (2011), assim como Fernandez (2023) enfatizam o reconhecimento facial como uma tipa de identificação biométrica antiga e, geralmente utilizado em aplicações forenses, ainda que elucidam a sua automação como evento recente.
[12] A retina, localizada na parte posterior do olho, é amplamente vascularizada e possui células fotorreceptoras (Graziano; Leone, 2005; Fernandez, 2023).
[13] É classificado como um método primário de identificação humana pela Interpol (Daruge; Daruge Júnior; Francesquini Júnior, 2017; Fernandez, 2023).
[14] Segundo Fernandez (2023), nesta forma de identificação humana as características comportamentais utilizadas na biometria representam medida como a forma de andar e a voz.
[15] Os sistemas biométricos analisam a pressão, velocidade, ritmo, sequência de formação das letras na escrita (Fernandez, 2023).
[16] Este método é uma tecnologia de identificação digital que verifica usuários de forma invisível, analisando a interação física com dispositivos online, como movimento do telefone, toque na tela ou ritmo de digitação (LexisNexis Risk Solutions, 2024).

Uma abordagem que para Fernandez (2023), agrega vantagens operacionais e funcionais da biometria: aumenta a segurança, diminui as possibilidades de fraude e permite o controle da própria identidade e o acesso à serviços com maior praticidade. No Brasil, por exemplo, o Tribunal Superior Eleitora (TSE**)** e a Polícia Federal (PF) têm sido exemplos e testemunhos de instituições que tem feito investimentos robustos em identificação digital humana através da biometria.

Esta realidade exposta descreve a necessidade consciente de identificação humana virtual para segurança de informação, visto que inibe a vulnerabilidade às ameaças de ataques cibernéticos e ou a sua potencial materialização como crime cibernético. E, como destaca IBM (2023), com o aumento de ataques cibernéticos, a autenticação multifatorial (MFA) tornou-se padrão em ambientes corporativos e bancários, elevando o nível de proteção contra invasões.

C. Tipos de Biometrias na identificação digital:

A revisão literária permitiu constatar a existência de distintos tipos de biometrias, sendo que cada uma delas tem suas respectivas caraterísticas e aplicações: impressões digitais, reconhecimento facial, reconhecimento da íris e retina, caligrafia[17], DNA[18], sistema auditivo e odor[19]. Porém, segundo Holder, Robinson e Laub (2011), as biometrias mais usadas na identificação digital são as impressões digitais, o

[17] Para Miranda, Harris, Brasil e O'Connell (2007) o sistema de identificação digital por caligrafia representa um dos tipos de Sistemas biométricos que analisam a pressão, velocidade, ritmo e sequência de formação das letras, e não apenas o formato. A geometria da Mão mede o comprimento, espessura e forma dos dedos (Fernandez, 2023).

[18] Um método fornece informações biométricas compactas, com baixo erro e alta precisão (Fernandez, 2023). E Brasil (2013, 2017, 2018, 2019), assim como Fernandez (2023) destacam que o Brasil possui um Banco Nacional de Perfis Genéticos (BNPG) e a Rede Integrada de Bancos de Perfis Genéticos (RIBPG), com mais de 27.000 perfis armazenados. Elementos estes, que permitem a execução deste método de identificação digital, considerando a existência de dados por processar. E a identificação digital através do DNA detém uma importante vantagem na identificação criminal, as sequências utilizadas não codificam proteínas, evita a revelação de traços somáticos ou comportamentais, o que o torna compatível com a Lei 12.654/2012 (Brasil, 2012; Fernandez, 2023)

[19] As impressões de orelha, como método de identificação digital, existem, em investigações forenses desde 1965. Mas, os estudos e técnicas ainda são considerados imaturos (Meijerman; Thean; Maat, 2005). E quanto aos Odores, de decomposição, estes podem ser percebidos por cães ou monitorizados por técnicas analíticas (Paczkowski; Schütz, 2011; Furton., 2015; Iqbal, 2017; Statheropoulos; Spiliopoulou; Agapiou, 2005). Ainda que, o Odor não possa representar uma forma de identificação digital, se condira uma abordagem ilustrativa dos tipos de identificação em segurança pública.

reconhecimento facial e, mais recentemente (2020-2025), o reconhecimento da íris e retina.

i. Impressões digitais

As impressões digitais têm sido amplamente utilizadas na identificação civil e criminal, na elucidação de crimes e na identificação de vítimas de desastres (Hawthorne, Plotkin e Douglas 2008; Fernandez, 2023)[20].

E no Brasil, por exemplo, atendendo a sua realidade criminal, segundo a Assessoria de Comunicação do Tribunal Superior Eleitoral (TSE)[21] (2017), o país investiu mais de R$ 127 milhões na individualização do eleitorado por biometria. Uma evidência que expõe esta necessidade de identificação digital como mecanismo de segurança cibernética. Realidades que, para Polícia Federal (PF, 2018), Ribeiro (2019) e Fernandez (2023), fazem parte dos esforços de instituições de segurança pública, como a Polícia Federal (do Brasil) no processo de modernização do seu sistema de segurança. Incluindo a comparação automatizada do reconhecimento facial à análise das impressões digitais e palmares[22]. Destacando a sua pertinência na perícia criminal, Holder, Robinson & Laub (2011), Hawthorne, Plotkin & Douglas (2008) e Fernandez (2023) enfatizam que este método pode indicar ou não a presença de um suspeito na cena do crime, sendo úteis também para corroboração civil e identificação de vítimas de desastres.[23]

ii. O reconhecimento facial

---

[20] Impressão Digital (Papiloscopia) são Minúcias, como terminações e bifurcações de cristas.[20] Seundo Fernandez (2023), este é o método mais bem-sucedido e popular para identificação de pessoas.
[21] A Sigla TSE significa Tribunal Superior Eleitoral (TSE) do Brasil e, é o Órgão máximo da Justiça Eleitoral no País.
[22] A esta abordagem da PF, Ratha e Govindaraju (2008), assim como Marcialis, Roli e Tidu (2010) alertam que a identificação digital tem vulnerabilidades que devem ser fortalecidas, enfatizando que, mesmo os sensores de contato e os *touchless* são suscetíveis a ataques de falsificação, inclusive com imagens 2D.
[23] Quase todas as agências policiais dependem de sistemas automatizados de identificação de impressões digitais (AFIS) (JAIN, ROSS & NANDAKUMAR, 2011a; MALTONI, 2009; Fernandez, 2023). Por exemplo, A Polícia Federal (2018) E Ribeiro (2019) elucida, que Polícia Federal do Brasil atualizou o seu sistema AFIS para um Sistema Automatizado de Identificação Biométrica (ABIS), incluindo autenticações como o reconhecimento facial e impressões palmares.

O reconhecimento facial é uma abordagem de identificação que, segundo Lima (2021), tem sido a tecnologia prioritária para muitas instituições bancárias no combate a fraudes. Fato que, segundo o autor, tem fundamentado o seu valor potencial para a segurança pública. E, por assim ser, o mercado da tecnologia de identificação digital (biometria facial) tem crescido com muito potencial agregado.

E para Duarte (2021) prevalece a necessidade de atenção redobrada no uso de tecnologias de biometria, como sistemas de reconhecimento facial automatizado para a segurança pública. Porque, segundo o autor, existe o risco potencial de privação de liberdade dos usuários. Um alerta que o autor o faz destacando, por exemplo, casos de sucesso e insucesso do seu uso no Brasil, que os comenta no escopo de debate sobre os limites da tecnologia em sociedades digitais. Tudo em referência aos antecedentes históricos, que recalcam a necessidade de considerar outros vários espectros emergentes em esforços semelhantes de garantia de segurança digital através do dométodo. Entre os precedentes legais, víeis (étnico-raciais) e estereótipos emergentes na aplicação destes métodos de identificação digitais no Brasil.

A esta exposição dos principais métodos identificação humana digital, também se destaca o reconhecimento da Íris e Retina (íris). Uma tecnologia que, segundo Al-Raisi e Al-Khouri (2008), bem como Fernandez (2023) detém uma das características biométricas mais precisas e, que carregam um alto volume de informações. Jain, Bolle e Pankanti (2006) expõem que os padrões de vasos sanguíneos da retina são considerados altamente estáveis devido à sua localização segura no olho. E para Al-Raisi e Al-Khouri (2008), junto a Fernandez (2023), este método de identificação digital é usado em aeroportos, controle de segurança, smartphones e contas bancárias. Tendo os seus padrões de confiabilidade que podem impactar sobremaneira neste nível de eficácia na identificação digital.

iii. Desafios e Preocupações da Biometria

A exposição dos distintos métodos e mecanismos de identificação humana na era digital, frequentemente referenciado como identificação digital, permite entender mais sobre as potencialidades destes mecanismos para a segurança digital no espaço cibernético e o seu potencial uso na segurança pública. Ainda assim, importante destacar que a identificação humana como mecanismo preventivo de contenção de ameaça digital no espaço cibernético também se caracteriza com desafios e preocupações como o da privacidade e consentimentos legais, acurácia, viés, vulnerabilidade a ataques, sistemas multibiométricos, etc.

Se por um lado, a identificação digital através do uso de biometrias levanta questões sobre privacidade, especialmente a venda e segurança de grandes bases de dados biométricos (Real, 2025): onde Brasil (2018) e EU 2016/679 (2016) consideram, através da Lei Geral de Proteção de Dados (LGPD) no Brasil e o Regulamento Geral sobre a Proteção de Dados (RGPD) na União Europeia, que os dados biométricos como sensíveis e estes que estabelecem e, o consentimento para o tratamento desses dados deve ser livre, informado e inequívoco, e o silêncio ou opções pré-validadas não configuram consentimento.[24]

Mesmo às exceções, Duarte (2021) enfatiza que a aplicação de reconhecimento facial em segurança pública deve basear-se em métodos técnico-científicos que respeitem princípios como unicidade, imutabilidade e perenidade. Uma abordagem que Duarte (2021) e Cóbe (2020) desenvolvem como solução ideal na construção de convergência entre o que chamam de "máquina e humano", sendo máquinas os sistemas automatizados que atuam como ferramentas auxiliares da atuação pericial humana que evite resultados enviesados e discriminações.

Por outro lado, se consideram potenciais equívocos de acurácia e viés, destes mecanismos de identificação humana. Por exemplo, Duarte (2021) refere que a tecnologia de reconhecimento facial pode apresentar vieses e imprecisões em relação

[24] Ainda que a LGPD no Brasil e o RGPD da União Europeia apresentem esta aclamação ética na identifição humana, Brasil (2018), Duarte (2021) e Cóbe (2020), igualmente destacam que, existem exceções ao exposto, para fins de segurança pública e investigação criminal. Ainda que o que exista debates jurídicos sobre a validade e limites dessas técnicas.

a dados demográficos, com taxas de erro significativamente mais altas para mulheres negras do que para homens brancos[25].

Ademais, a vulnerabilidade a ataques cibernéticos também representa parte dos desafios atuais na identificação humana através da biometria. Ainda que, no determinado momento, Mordini e Tzovaras (2012), assim como Ratha, Connell e Bolle (2001) enfatizem que, os sistemas biométricos são suscetíveis a ataques de apresentação (*spoofing*) com amostras falsas ou ataques internos, estas realidades crescem com a sofisticação dos crimes. Fato que denota a necessidade crescente de, igualmente, sofisticação de criptografia em processos de identificado digital que demostre ser mais seguro e eficiente a ataques externos.

A esta realidade exposta, a abordagem de sistemas multibiométricos pode resultar ser a mais eficiente e eficaz na superação desafios similares aos citados na identificação humana. Isso, considerando que, por exemplo, Jain, Flynn e Ross (2007), assim como Ross, Nandakumar e Jain (2006), já haviam destacado que, a combinação de múltiplas características biométricas (como impressões digitais, face e íris) para superar as limitações de traços únicos, aumentam, significativamente, a precisão e a unicidade da identificação. Uma abordagem que vai mais além do duplo fator, muito mais adaptado na identificação digital atualmente (2025).

2.4. GOVERNANÇA DE DADOS, SOBERANIA INFORMACIONAL E GEOPOLÍTICA DA IDENTIDADE

a) A Quem Pertencem os Dados da Identidade Digital?

A pergunta central no debate sobre identidade digital é: quem detém o controle dos dados que definem o sujeito online? A resposta, infelizmente, não é o próprio usuário. A maioria dos dados é coletada por empresas privadas, processada

[25] Junto a abordagem supracitada, existe a abordagem de Sumares (2018) que indica que o reconhecimento facial policial errou 92% das vezes em um evento. Uma realidade que, atualmente, pode representar outra realidade, considerando o advento da inteligência artificial mais optimizada. Ainda que esta incidência demostra a necessidade de contínuo desenvolvimento algorítmico para o melhoramento deste método biométrico de identificação humana, principalmente, na identificação criminal.

por servidores em outras jurisdições e protegida por contratos opacos de termos de uso.

Segundo Zuboff (2018, p. 143), "os dados pessoais não são mais apenas registros administrativos, mas recursos estratégicos de poder econômico e político". Eles se tornaram o novo petróleo da economia global, gerando assimetrias profundas entre usuários, plataformas e Estados.

A soberania informacional — isto é, a capacidade de um país garantir que os dados de seus cidadãos sejam tratados conforme seus próprios valores e leis — torna-se um imperativo político diante da interdependência digital e da concentração de poder em poucas big techs.

b) Modelos Internacionais de Identificação e Controle

Diversos países adotaram modelos distintos de governança da identidade digital:

- **Estônia**: desenvolveu um sistema de identidade digital nacional (e-Residency) que permite total controle do cidadão sobre seus dados e acesso universal a serviços digitais do governo.

- **União Europeia**: com o GDPR, estabelece uma estrutura robusta de proteção de dados e direitos individuais.

- **China**: utiliza a identidade digital integrada a um sistema de vigilância em larga escala, com pontuação social que interfere em mobilidade, crédito e acesso a benefícios.

- **Índia**: criou o Aadhaar, maior sistema de identificação biométrica do mundo, mas enfrenta críticas por falta de consentimento adequado e riscos de exclusão social.

O Brasil, com a LGPD e o Marco Civil da Internet, tem bases legais para promover um modelo democrático de proteção da identidade digital. No entanto,

ainda carece de fiscalização efetiva, estrutura de governança sólida e cultura de transparência algorítmica (BRASIL, 2014; 2018).

CONSIDERAÇÕES FINAIS

A revolução tecnológica deste século tem movimentado o planeta em praticamente todos os segmentos. Não há como recuar aos avanços e progressos obtidos pela sociedade com a popularização da internet. Por outro lado, há uma crescente preocupação em relação à segurança no denominado ambiente cibernético.

Os ataques cibernéticos elevaram substancialmente o número de crimes cometidos no ambiente virtual. Assim sendo, a vulnerabilidade à esses ataques, impulsionou empresas e instituições a investirem em segurança tecnológica visando um espaço mais seguro.

Nesse contexto, os processos de identificação humana surgem como uma alternativa para o aumento da segurança em rede. Diferente da identidade, atributo intrínseco da pessoa, a identificação é o processo técnico de autenticação e verificação que possibilita distinguir indivíduos e garantir acessos de forma segura.

Ressalta-se que os mecanismos de identificação demandam cautela, principalmente porque envolvem aspectos éticos, jurídicos e sociais, sobretudo quanto à privacidade e tratamento de dados sensíveis. A identificação digital é uma representação algorítmica do sujeito, que pode ser usada para oferecer serviços, mas também para manipular, discriminar e excluir, além da exposição e violações de direitos fundamentais.

Os riscos à identidade digital não se limitam aos vazamentos de dados, mas incluem: vigilância em massa, manipulação comportamental, discriminação algorítmica, supressão de direitos, perda de autonomia informativa, dentre outros que afrontam os direitos fundamentais do indivíduo.

A proteção à identidade digital exige articulação estruturada que inclua: uma legislação eficiente e atualizada; regulação das plataformas e algoritmos; desenvolvimento de ferramentas técnicas de proteção (criptografia, firewalls, autenticação avançada) e formação de uma cidadania crítica e empoderada capaz de superar os perigos cibernéticos.

A identidade no ciberespaço é o novo campo de disputa pelo poder simbólico, social e político. Defender a integridade dessa identidade é defender o direito de existir como sujeito pleno no século XXI.

4 REFERÊNCIAS

REFERÊNCIAS BIBLIOGRAFICAS

- AL-RAISI, Ahmad N.; AL-KHOURI, Ali M. Iris recognition and the challenge of homeland and border control security in UAE. *Telematics and Informatics*, v. 25, n. 2, p. 117-132, 2008.

- BRASIL. Como funciona a biometria. Disponível em: http://ciencia.hsw.uol.com.br/bometrica1.htm. Acesso em: ago. 2025.

- BRASIL. Lei n. 12.965, de 23 de abril de 2014: Marco Civil da Internet. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

- BRASIL. Lei n. 13.709, de 14 de agosto de 2018: Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

- BRASIL. Secretaria de Segurança da Informação e Cibernética. *Autenticação de dois fatores*. Brasília, DF: GSI/PR, [2024]. (Fascículo Manual de Segurança Digital). Acesso em: 17 ago. 2025.

- CASTELLS, Manuel. *A sociedade em rede*. 6. ed. São Paulo: Paz e Terra, 2003.

- CÓBE, Raphael M. O.; NONATO, Luiza G.; NOVAES, Sérgio F.; ZIEBARTH, José A. Rumo a uma política de Estado para inteligência artificial. *Revista USP*, n. 124, p. 37-48, 2020. Disponível em: https://www.revistas.usp.br/revusp/article/view/167914. Acesso em: 8 set. 2025.

- COMISSÃO EUROPEIA. Entrada em vigor do Regulamento Identidade Digital. *Shaping Europe's digital future*, 21 maio 2024. Disponível em: https://digital-strategy.ec.europa.eu/pt/news/entry-force-digital-identity-regulation. Acesso em: 17 ago. 2025.

- DARUGE, Eduardo; DARUGE JÚNIOR, Eduardo; FRANCESQUINI JÚNIOR, Luiz. *Tratado de odontologia legal e deontologia*. Curitiba: Santos, 2017.

- DUARTE, Renata et al. Aplicação dos sistemas biométricos de reconhecimento facial na segurança pública. *Brazilian Journal of Forensic Sciences, Medical Law and Bioethics*, v. 11, n. 1, p. 1-21, 2021.

- FERNANDEZ, Ramon Santos et al. *Biometrias: das teorias às aplicações*. Brasília, DF: ANP Editora, 2023.

- GATES, Bill. *The road ahead*. New York: Viking Press, 2005.

- GIL, Antonio Carlos. Como Elaborar Projetos de Pesquisa. 5. ed. São Paulo: Atlas, 2010.

- GRAZIANO, Rosa Maria; LEONE, Cléa Rodrigues. Frequent ophthalmologic problems in premature infants. *J. Pediatr.*, v. 81, n. 4, p. 285-290, 2005.

- HADNAGY, Christopher. *Social engineering: the science of human hacking*. Indianapolis: Wiley, 2018.

- HARRIS, Tom. Como funcionam os leitores de impressões digitais. Disponível em: http://www.uol.com.br/leitores-de-impressoes-digitais.htm. Acesso em: ago. 2007.

- HAWTHORNE, Mark R.; PLOTKIN, Sharon L.; DOUGLAS, Bracey-Ann. *Fingerprints: analysis and understanding the science*. Boca Raton: CRC Press, 2008.

- HOLDER, Eric H.; ROBINSON, Laurie O.; LAUB, John H. *The fingerprint sourcebook*. Washington, DC: National Institute of Justice, 2011.

- IBM. *X-Force Threat Intelligence Index 2023*. Disponível em: https://www.ibm.com/reports/threat-intelligence.

- IQBAL, Mohammad A. et al. Forensic decomposition odour profiling: a review of experimental designs and analytical techniques. *TrAC Trends in Analytical Chemistry*, v. 91, p. 112-124, 2017. Disponível em: https://pubmed.ncbi.nlm.nih.gov/24582974/. Acesso em: 20 jul. 2021.

- JAIN, Anil K.; BOLLE, Ruud M.; PANKANTI, Sharath (org.). *Biometrics: personal identification in networked society*. Nova Iorque: Springer US, 2006.

- JAIN, Anil K.; CHEN, Yi; DEMIRKUS, Meltem. *Pores and ridges: fingerprint systems*. Nova Iorque: Springer US, 2007.

- JAIN, Anil K.; DASS, Sarat C.; NANDAKUMAR, Karthik. Soft biometric traits for personal recognition systems. In: ZHANG, David Y.; JAIN, Anil K. (eds.). *ICBA 2004: Biometric Authentication*. Berlim: Springer, 2004. p. 731-738.

- LEXISNEXIS RISK SOLUTIONS INC. *Menos fraudes com biometria comportamental*. [S.l.]: LexisNexis, 2024. Acesso em: 17 ago. 2024.

- LIMA, Fabiana. Por que sua empresa precisa investir em biometria facial? *Idblog*, 03 fev. 2021. Disponível em: https://blog.idwall.co/investir-em-biometria-facial. Acesso em: 10 ago. 2025.

- MARCIALIS, Gian Luca; ROLI, Fabio; TIDU, Alessandra. Analysis of fingerprint pores for vitality detection. In: *INTERNATIONAL CONFERENCE ON PATTERN RECOGNITION*, 20., 23-26 ago. 2010, Istambul, Turquia. Proceedings… Istambul: IEEE, 2010. Disponível em: https://doi.org/10.1109/icpr.2010.321. Acesso em: 10 ago. 2025.

- MEIJERMAN, Lynn; THEAN, Andrew; MAAT, George. Earprints in forensic investigations. *Forensic Science, Medicine and Pathology*, v. 1, n. 4, p. 247-256.

- MINAYO, Maria Cecília de Souza. O Desafio do Conhecimento: Pesquisa Qualitativa em Saúde. 14. ed. São Paulo: Hucitec, 2014.

- MIRANDA, Leonel. Biometria: o que é e o que faz? Disponível em: http://www.sinfic.pt/SinficNewsletter/index.html. Acesso em: ago. 2025.

- MORDINI, Emilio; TZOVARAS, Dimitros. *Second generation biometrics: the ethical, legal and social context*. Nova Iorque: Springer, 2012.

- NATIONAL CYBER SECURITY CENTRE – NCSC. *Annual Review 2022*. Londres, 2022. Disponível em: https://www.ncsc.gov.uk.

- NEUROTECH. Como a biometria facial ajuda a combater fraudes de identidade. [S.l.]: Neurotech, 2024.

- O'CONNELL, Ann Meeker. Como funcionam as evidências de DNA. Disponível em: http://ciencia.hsw.uol.com.br/evidencias-de-dna.htm. Acesso em: ago. 2025.

- PACZKOWSKI, Sebastian; SCHÜTZ, Stefan. Post-mortem volatiles of vertebrate tissue. *Applied Microbiology and Biotechnology*, v. 91, n. 4, p. 917-935, 2011. Disponível em: http://dx.doi.org/10.1007/s00253-011-3417-x.

- PROTIVITI INC. *Além das senhas: como a autenticação reforça a postura de segurança cibernética*. [S.l.]: Protiviti Inc. Acesso em: ago. 2025.

- RATHA, Nalini K.; GOVINDARAJU, Venu (eds.). *Advances in Biometrics: sensors, algorithms and systems*. Nova Iorque: Springer, 2008.

- REAL, Fernanda. Biometria facial não é totalmente segura, mas possui mais vantagens que desvantagens. São Carlos: Portal USP São Carlos.

- REGULAMENTO (UE) 2016/679 do Parlamento Europeu e do Conselho. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. 27 abr. 2016. Disponível em: https://gdpr-info.eu. Acesso em: ago. 2025.

- RIBEIRO, Caroline L. *Estudo acerca da modernização do sistema automatizado de impressões digitais da Polícia Federal - AFIS/PF*. Brasília: Escola Superior de Polícia – ANP, 2019.

- SANTOS, Natalia. Por que a identidade é a primeira linha de defesa da segurança cibernética. [S.l.]: Sec4You, 1 mar. 2023. Acesso em: 17 ago. 2025.

- SILVA, Clevertom et al. *A segurança através da biometria*. [S.l.]: Associação Educacional Dom Bosco (AEDB), [2007]. Disponível em: [URL não fornecida]. Acesso em: 17 ago. 2025.

- STATHEROPOULOS, M.; SPILIOPOULOU, C.; AGAPIOU, A. A study of volatile organic compounds evolved from the decaying human body. *Forensic Science International*, v. 153, n. 2-3, p. 147-155, 2005. Disponível em: http://dx.doi.org/10.1016/j.forsciint.2004.08.015. Acesso em: ag. 2025.

- SUMARES, G. Reconhecimento facial policial da Champion's League errou 92 % das vezes. *Olhar Digital*, 08 maio 2018. Disponível em: https://olhardigital.com.br/fique_seguro/noticia/reconhecimento-facial-policial-confundiu-2300-pessoas-com-potenciais-criminosos/75918.

- TRIBUNAL SUPERIOR ELEITORAL. Assessoria de Comunicação. TSE e Polícia Federal vão compartilhar banco de dados biométricos. *Tribunal Superior*

Eleitoral, 16 nov. 2017. Disponível em: http://www.tse.jus.br/imprensa/noticias-tse/2017/Novembro/tse-e-policia-federal-vao-compartilhar-banco-de-dados-biometricos.

- ZUBOFF, Shoshana. *The age of surveillance capitalism: the fight for a human future at the new frontier of power*. New York: Public Affairs, 2018.