SEGURANÇA E VIOLÊNCIA NO MEIO DIGITAL: RISCOS, LACUNAS INSTITUCIONAIS E ESTRATÉGIAS DE MITIGAÇÃO

SAFETY AND VIOLENCE IN THE DIGITAL ENVIRONMENT: RISKS, INSTITUTIONAL GAPS AND MITIGATION STRATEGIES

SEGURIDAD Y VIOLENCIA EN EL ENTORNO DIGITAL: RIESGOS, BRECHAS INSTITUCIONALES Y ESTRATEGIAS DE MITIGACIÓN

10.56238/IIMultiCientifica-132

Ana Carla Nunes do Nascimento Santos
Instituição: Instituto Federal de Educação Ciência e Tecnologia do Sertão Pernambucano (IFSERTÃO)
Lattes: http://lattes.cnpq.br/4078359580398724
E-mail: anacarlanunes907@gmail.com
Orcid: https://orcid.org/0009-0000-9806-5096

RESUMO
Este artigo analisa segurança e violência no ambiente digital, objetivando mapear mecanismos de amplificação, lacunas institucionais e medidas de mitigação. Com metodologia de revisão bibliográfica e análise documental qualitativa (codificação temática e triangulação), investiga como arquiteturas de plataformas, modelos de IA e dinâmicas econômicas potencializam práticas abusivas — entre elas deepfakes, divulgação íntima não consensual e assédio — e fragilizam a proteção de usuários, especialmente grupos vulneráveis. Resultados apontam que governança de TI, controles técnicos, resposta a incidentes e letramento digital são essenciais para prevenção, detecção e apoio a vítimas, recomendando ações integradas entre plataformas, Estado e sociedade para promoção de direitos.

Palavras-chave: Segurança Digital. Violência Digital. Governança de TI. Inteligência Artificial. Letramento Digital.

ABSTRACT
This article analyzes security and violence in the digital environment, aiming to map amplification mechanisms, institutional gaps, and mitigation measures. Using a methodology of bibliographic review and qualitative documentary analysis (thematic coding and triangulation), it investigates how platform architectures, AI models, and economic dynamics potentiate abusive practices — among them deepfakes, non-consensual intimate disclosure, and harassment — and weaken user protection, especially for vulnerable groups. Results indicate that IT governance, technical controls, incident response, and digital literacy are essential for prevention, detection, and victim support, recommending integrated actions among platforms, State, and society to promote rights. Keywords: digital security; digital violence; IT governance; artificial intelligence; digital literacy.

Keywords: Digital Security. Digital Violence. IT Governance. Artificial Intelligence. Digital Literacy.

RESUMEN
Este artículo analiza la seguridad y la violencia en el entorno digital, con el objetivo de mapear mecanismos de amplificación, brechas institucionales y medidas de mitigación. Con una metodología de revisión bibliográfica y análisis documental cualitativo (codificación temática y triangulación), investiga cómo las arquitecturas de plataformas, los modelos de IA y las dinámicas económicas potencian prácticas abusivas — entre ellas deepfakes, divulgación íntima no consensual y acoso — y debilitan la protección de usuarios, especialmente grupos vulnerables. Los resultados indican que la gobernanza de TI, los controles técnicos, la respuesta a incidentes y la alfabetización digital son esenciales para la prevención, detección y apoyo a víctimas, recomendando acciones integradas entre plataformas, Estado y sociedad para la promoción de derechos. Palabras clave: seguridad digital; violencia digital; gobernanza de TI; inteligencia artificial; alfabetización digital.

Palabras clave: Seguridad Digital. Violencia Digital. Gobernanza de las Tecnologías de la Información. Inteligencia Artificial. Alfabetización Digital.

1 INTRODUÇÃO

A complexidade das interações contemporâneas exige uma reestruturação do olhar sobre o ambiente digital, onde a segurança transcende a esfera meramente técnica e passa a ser uma questão de consciência cognitiva sobre a própria vulnerabilidade. Ao compreender que os riscos de assédio e exposição não são fatos isolados, mas elementos estruturais desse ecossistema, o usuário desenvolve mecanismos de defesa mais resilientes. Com a mudança de paradigma transforma a passividade diante da tecnologia em uma postura estratégica, na qual o letramento e a vigilância constante deixam de ser um ônus para se tornarem pilares fundamentais de autonomia, garantindo que o espaço virtual funcione como um ambiente de expressão e não como uma ameaça constante. Com isso, a tecnologia é um servidor útil, mas um mestre perigoso, alertou Christian Lous Lange ainda em (1921). Essa máxima define, com precisão, o paradoxo da contemporaneidade, enquanto as ferramentas de conectividade encurtaram distâncias e democratizaram a informação, elas também gestaram novos e sofisticados mecanismos de opressão. Ao longo desse processo, a internet consolidou-se como o primeiro espaço onde a humanidade tem a capacidade de compartilhar tudo, mas também onde temos a responsabilidade de filtrar o que realmente nos protege (WORLD WIDE WEB FOUNDATION, 2019). Nesse cenário, a vigilância torna-se o custo que pagamos pela conveniência da era digital (Schneier, 2015). Por essa razão, esse paradoxo atingiu um patamar crítico em 2025, pois a tecnologia deixou de ser uma ferramenta de apoio para tornar-se um ambiente arquitetônico, onde a conveniência muitas vezes atua como o véu que encobre a perda da soberania digital do indivíduo (TECH ETHICS INSTITUTE, 2025). Ademais, tal cenário revela-se , essa realidade é particularmente alarmante no que tange às violências de gênero, pois, como aponta a ONU Mulheres (2025), a violência digital de gênero deixou de ser um subproduto das redes sociais para se tornar uma estrutura sistemática de controle, exigindo uma resposta jurídica e técnica integrada.A relevância desta pesquisa justifica-se pela necessidade premente de decodificar as novas dinâmicas de vulnerabilidade que surgiram nesse ecossistema digital. Do ponto de vista teórico, a contribuição deste trabalho reside em integrar reflexões clássicas sobre ética tecnológica com os desafios contemporâneos da soberania digital, propondo uma reestruturação do olhar acadêmico que transcende a segurança meramente técnica. O estudo articula a consciência cognitiva como elemento central para a compreensão da violência de gênero estrutural, avançando o debate sobre a autonomia do usuário. Na esfera prática, a pesquisa contribui ao fornecer diretrizes para o letramento digital estratégico, transformando o conhecimento em mecanismos de defesa resilientes. Ao demonstrar que a vigilância constante e o letramento são

pilares de proteção, o trabalho oferece aos usuários e profissionais ferramentas para mitigar riscos, incentivando a transição de uma postura passiva para uma atuação estratégica e segura no ambiente virtual.Nesse contexto, a complexidade das interações contemporâneas exige que a segurança seja encarada como uma questão de consciência cognitiva sobre a própria vulnerabilidade. Diante disso, o objetivo geral deste artigo é analisar o paradoxo da tecnologia como ferramenta de opressão e proteção, identificando estratégias que permitam ao usuário transformar sua postura diante do ambiente virtual, garantindo que o espaço digital funcione como um ambiente de expressão, acolhimento e denúncia, e não como uma ameaça constante.

2 PASSOS METODOLÓGICOS

Como procedimentos metodológicos, realizou-se revisão bibliográfica e análise documental qualitativa, integrando artigos acadêmicos, relatórios institucionais e fontes jornalísticas sobre segurança e violência digital. Foram priorizadas obras de referência, entre elas Mello (2020) — violência digital e desinformação; Grelin (2026) — IA e geração de imagens íntimas não consensuais; relatórios do UNODC e da ONU Mulheres — enquadramento institucional e gênero; estudos do Oxford Internet Institute — ecossistema de geradores de deepfake; e textos de Schneier (2015) sobre vigilância e arquitetura tecnológica.

Quanto à seleção das fontes, as fontes foram selecionadas por relevância temática, atualidade e autoridade. Procedeu-se codificação temática (segurança pessoal e digital, amplificação algorítmica, deepfakes/nudificação, impacto de gênero, respostas institucionais) e triangulação entre diferentes tipos de evidência para construir uma síntese interpretativa.Quanto à sua natureza, estudo de caráter descritivo-interpretativo, sem intenção de quantificação, limitações incluem disponibilidade de fontes e vieses de publicação.

3 PERSPECTIVAS TEÓRICAS

3.1 SEGURANÇA NO AMBIENTE DIGITAL

Sob essa ótica inicial, a segurança no ambiente digital transcende a mera proteção técnica contra ameaças cibernéticas, configurando-se como um dos pilares fundamentais da cidadania contemporânea. Em um cenário onde a tecnologia está intrinsecamente ligada ao acesso à informação e à interação social, a compreensão sobre o uso responsável, a ética e a observância de normas como a LGPD torna-se indispensável. Promover a segurança digital, portanto, não é apenas um mecanismo

de defesa contra riscos e fraudes, mas um compromisso educativo essencial para garantir a integridade, a autonomia e a confiança dos usuários em uma sociedade cada vez mais conectada**.** A Partir dessa perspectiva, a segurança tecnológica vai muito além de uma simples barreira técnica, ela constitui o alicerce indispensável que sustenta a confiança necessária, assegura a integridade absoluta das informações sensíveis e viabiliza a continuidade ética de todos os serviços essenciais no mundo digital (Reis *et al.* (2025). Com isso, a segurança na tecnologia é o que sustenta a vida digital hoje. Sem ela, a inovação perde o seu valor porque o risco se torna maior que o benefício. Conforme apontam Araújo *et al.* (2024), a promoção da segurança digital não apenas instrumentaliza o indivíduo contra riscos e fraudes, mas atua como um fator crucial para fortalecer a autonomia e a autoestima de populações vulneráveis, como as mulheres idosas, permitindo uma inserção mais confiante e ativa no mundo tecnológico. Somando a isso, a promoção da cidadania digital e a observância da LGPD são elementos essenciais para a construção de ambientes educacionais mais seguros, éticos e inclusivos, capazes de assegurar a proteção de dados e o uso responsável das tecnologias na educação contemporânea (Figueiredo, 2026). Do mesmo modo, "a formação de cidadãos digitais responsáveis torna-se uma necessidade premente, exigindo uma abordagem ativa para equilibrar os benefícios da tecnologia com a responsabilidade de seu uso seguro e ético." (Venâncio *et al.*, 2024, P. 5 apud França *et al.*, 2025). E conseguentimente, a segurança online requer a adoção de práticas e medidas de proteção para reduzir ataques e preservar a confiança dos usuários, sobretudo diante do crescente uso da internet para transações comerciais e entretenimento (De Oliveira, 2026)

3.2 VIOLÊNCIA DIGITAL

Sob essa perspectiva inicial, a violência digital constitui uma forma contemporânea de agressão que pode causar impactos profundos na vida das vítimas. Além dos danos emocionais, suas consequências podem afetar a rotina, a saúde física e a segurança das pessoas atacadas. Rivelli (2025) destaca que práticas como perseguição online, instalação de software espião, divulgação íntima sem consentimento e difamação geram danos psicológicos, compromissos no funcionamento diário e repercussões físicas às pessoas atacadas, o que demanda respostas jurídicas e políticas públicas integradas e flexíveis. Além disso, a rápida evolução tecnológica amplifica essas ameaças, pois ferramentas digitais e algoritmos facilitam a vigilância, a disseminação e o rastreamento das vítimas. Em relação a esse fenômeno, a segurança e a violência digital estão entrelaçadas, as mesmas tecnologias que ampliam acesso e oportunidades também criam novos caminhos para abuso, controle

e dano (UNODC — ESCRITÓRIO REGIONAL DO UNODC PARA A ÁFRICA AUSTRAL, s.d.). Partindo dessa perspectiva, a IA e as plataformas digitais ampliaram a violência digital ao facilitar a criação, divulgação e promoção de conteúdos íntimos não consensuais, deepfakes e assédio, gerando danos psicológicos, sociais e riscos físicos, sobretudo para mulheres (Grelin,2026).Considerando esse aspecto, De Oliveira (2026) lembra que a proteção de dados pessoais é essencial, já que no espaço digital o furto de informações e atores mal-intencionados constituem riscos constantes. Em complemento, Maia e Costa (2023) destacam que os crimes cibernéticos, impulsionados pelo crescente uso da internet e pela evolução tecnológica, tornaram-se uma ameaça global que exige legislação atualizada, investimento em tecnologia e cooperação entre setor público e privado.Nesse contexto, Mello (2020) analisa como fake news e a violência digital, produzidas e amplificadas por atores organizados, plataformas e incentivos econômicos, alimentam intolerância e polarização, transformando a informação em arma que atinge reputações, incita ódio, causa danos sociais e pessoais e corrói a confiança pública e o debate democrático. Em respostas a esses desafios, a gestão de TI é crucial para a segurança digital, ao organizar políticas de proteção de dados, implementar controles técnicos e capacitar usuários para prevenir e mitigar esses ataques.(DO NASCIMENTO SANTOS,2026).

4 RESULTADOS

No contexto dessa discussão, a análise documental e bibliográfica revelou que a arquitetura das plataformas digitais e o uso de IA estruturam a violência digital. Recursos como automação, escalabilidade e anonimato facilitam a criação e a circulação de conteúdos abusivos, tornando o problema sistêmico.Com base nisso, observou-se que algoritmos e modelos econômicos ampliam essa violência. Sistemas de recomendação, APIs e estratégias de monetização favorecem a rápida disseminação de conteúdos sensacionalistas ou íntimos não consensuais.Perante essa realidade, foram identificadas formas recorrentes de violência digital, como deepfakes, divulgação íntima não consensual, doxxing, assédio e ameaças. Essas práticas provocam danos psicológicos, sociais e profissionais, além de riscos físicos e revitimização.Em face dessa situação, a segurança digital mostrou-se essencial para proteger dados, prevenir, detectar e responder a incidentes. A integração entre controles técnicos, resposta a incidentes e governança reduz a exposição e contribui para a mitigação dos danos.

Em relação a essa realidade, a gestão de TI e a segurança da informação atuam como fatores importantes de mitigação. Governança madura, controles técnicos, capacitação e protocolos de apoio às vítimas reduzem o tempo de exposição, aceleram as remoções e limitam os danos.Portanto, persistem fragilidades como detecção insuficiente, remoções lentas, cooperação limitada entre plataformas e autoridades, leis fragmentadas e baixo letramento digital. Além disso, por se basearem em evidências qualitativas e documentais, os resultados exigem cautela na generalização.

5 CONCLUSÃO

Conclui-se que a arquitetura das plataformas digitais e o uso de IA ampliam formas de violência digital, como deepfakes, divulgação íntima não consensual e campanhas de assédio. Favorecidos por algoritmos, monetização e anonimato, esses atos provocam danos psicológicos, sociais e físicos, sobretudo em grupos vulneráveis.Nesse sentido, a segurança digital é essencial para prevenir, detectar e responder a esses incidentes. A integração entre governança, controles técnicos e suporte às vítimas reduz a exposição e os impactos, enquanto falhas nesses elementos aumentam a vulnerabilidade dos usuários. Nesse contexto, os achados oferecem subsídios para políticas públicas e iniciativas civis, com foco em canais de denúncia acessíveis, letramento digital, apoio às vítimas, responsabilização das plataformas e cooperação internacional. Essas medidas podem orientar ações preventivas e educativas.Para a academia, o estudo destaca a necessidade de investigar a relação entre tecnologia e violência digital, avaliar ferramentas de detecção e analisar a governança de TI.

Recomenda-se uma abordagem interdisciplinar, envolvendo tecnologia, direito, ciências sociais e saúde mental.Em conclusão, reconhecem-se as limitações da análise qualitativa e documental, que não permite estimar a prevalência do fenômeno e pode apresentar vieses na seleção das fontes. Recomenda-se, portanto, a realização de pesquisas empíricas, quantitativas e longitudinais sobre revitimização, interseccionalidades e eficácia de medidas preventivas.

REFERÊNCIAS

ARAÚJO, Cindy VA *et al.* Tecnologia, segurança e autonomia: Relato de um curso de inclusão digital para mulheres da terceira idade. In: Women in Information Technology (WIT). SBC, 2025. p. 730-740.

BRASIL, Beatriz Silveira *et al.* A violência na prática de crimes no ciberespaço. Novos Cadernos NAEA, v. 20, n. 2, p. 127-148, 2017.

CAIXETA, Simone Aparecida Lavorato. SEGURANÇA E CIDADANIA DIGITAL: DIREITOS, DEVERES E DESAFIOS NO AMBIENTE EDUCACIONAL. Revista Educação

DE FRANÇA, Ervelany Lins *et al.* Navegando com Segurança: cartilha educativa de conscientização sobre segurança digital. In: Simpósio Brasileiro de Computação na Educação Básica (SBC-EB). SBC, 2025. p. 201-207.

DE OLIVEIRA, Joelma Linhares *et al.* VIOLÊNCIA DIGITAL CONTRA MENINAS FORA DO CONTEXTO ESCOLAR: UMA REVISÃO DE LITERATURA. Revista Tópicos , v. 4, nº. 34, pág. 1-31, 2026.

DE OLIVEIRA, Simone Maldonado Monteiro. SEGURANÇA DIGITAL NA CONTEMPORANEIDADE: PERSPECTIVAS DIÁLOGICAS EM FOCO. Revista Educação Contemporânea, v. 3, n. 1, p. 493-499, 2026.

DO NASCIMENTO SANTOS, Ana Carla Nunes. A IMPORTÂNCIA DA GESTÃO DE TI NA PROTEÇÃO DE DADOS E PRIVACIDADE NA ERA DIGITAL. Anais Eventos, 2026.

FIGUEIREDO, Simone Oliveira *et al.* Cidadania digital: caminhos para ambientes educacionais seguros e éticos. Revista Tópicos, v. 4, n. 29, p. 1-14, 2026.

GRELIN, Daniela. A Inteligência Artificial e o novo Cenário de Violência Digital [LinkedIn]. LinkedIn, s.d. Disponível em: https://www.linkedin.com/pulse/intelig%25C3%25AAncia-artificial-e-o-novo-cen%25C3%25A1rio-de-viol%25C3%25AAncia-daniela-grelin-0skpf/ . Acesso em: 21 ago. 2026.

LANGE, Christian Lous. Internationalism. 1921. Nobel Lecture, Nobel Prize Outreach AB, Estocolmo, 13 dez. 1921. Disponível em: https://www.nobelprize.org/prizes/peace/1921/lange/lecture/ . Acesso em: 18 ago. 2026.

MAIA, Karolline Barbosa; COSTA, Cezar Henrique Ferreira. Crimes cibernéticos. Revista Ibero-Americana de Humanidades, Ciências e Educação, v. 9, n. 10, p. 109-126, 2023.

MELLO, Patrícia Campos. A maquina do ódio: notas de um repórter sobre fake news e violência digital . Companhia das Letras, 2020.

ONU MULHERES. Tecnologia e violência de gênero: relatórios de proteção 2025. 2025. Disponível em: https://www.unwomen.org/pt/digital-safety-2025 . Acesso em: 18 ago. 2026

REIS, Zilma Silveira Nogueira *et al.* Qualidade de dados e segurança digital na APS: Educação permanente para pessoas na gestão da atenção primária à saúde, gerentes de unidades de saúde e profissionais de tecnologia digital de informação e comunicação. 2025.

RIVELLI, Fabio. A violência digital e seus efeitos nas vítimas: desafios contemporâneos e perspectiva do ser humano digital. Revista Internacional de Vitimologia e Justiça Restaurativa, v. 3, n. 1, 2025.

SCHNEIER, Bruce. Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. New York: W. W. Norton & Company, 2015. Disponível em: https://www.schneier.com/books/data-and-goliath/ . Acesso em: 18 ago. 2026.

TECH ETHICS INSTITUTE. The architecture of digital sovereignty. 2025. Disponível em: https://techethics.org/publications/2025/sovereignty . Acesso em: 18 ago. 2026.

UNODC — Escritório das Nações Unidas sobre Drogas e Crime. Violência digital. [S.l.], s.d. Disponível em: https://www.unodc.org/rosaf/mozambique/violencia-digital.html. Acesso em: 21 ago. 2026.

WORLD WIDE WEB FOUNDATION. Contract for the Web. 2019. Disponível em: https://contractfortheweb.org/ . Acesso em: 18 ago. 2026.