REVISTA TÓPICOS
ISSN 2965-6672 | Qualis A2

ARQUITETURA DIGITAL DA CIDADANIA: REPENSANDO A SEGURANÇA ONLINE NAS INSTITUIÇÕES EDUCACIONAIS

DIGITAL CITIZENSHIP ARCHITECTURE: RETHINKING ONLINE SECURITY IN EDUCATIONAL INSTITUIONS

Ciências Sociais Aplicadas • 13/02/2025

REGISTRO DOI: 10.5281/zenodo.14861970

Eunice Pereira Nikassa dos Santos[1]

Micael Campos da Silva[2]

RESUMO

Este trabalho aborda o tema da segurança digital e cidadania online nas instituições educacionais, discutindo a importância de integrar práticas seguras e responsáveis no uso da tecnologia no ambiente escolar. O objetivo principal é investigar como a segurança digital pode ser promovida nas escolas, além de explorar os desafios e ameaças relacionadas à cidadania digital. A pesquisa é de natureza qualitativa, com uma metodologia bibliográfica que envolve uma análise de literatura especializada sobre o tema. Foram considerados conceitos fundamentais da cidadania digital, os principais riscos no ambiente escolar, como cyberbullying e a exposição de dados pessoais, bem como as melhores práticas para promover a segurança digital. Como considerações finais, o estudo conclui que, embora a implementação de políticas e práticas de segurança digital seja essencial, a conscientização de toda a comunidade escolar, incluindo alunos, professores e pais, é crucial para garantir um ambiente educacional seguro e ético no contexto online.

Palavras-chave: Cidadania digital, Conscientização, Privacidade, Riscos cibernéticos, Segurança digital.

ABSTRACT

This paper addresses the topic of digital security and online citizenship in educational institutions, discussing the importance of integrating safe and responsible practices in the use of technology in the school environment. The main objective is to investigate how digital security can be promoted in schools, in addition to exploring the challenges and threats related to digital citizenship. The research is qualitative in nature, with a bibliographic methodology that involves an analysis of specialized literature on the subject. Fundamental concepts of digital citizenship, the main risks in the school environment, such as cyberbullying and the exposure of

personal data, as well as best practices to promote digital security were considered. As final considerations, the study concludes that, although the implementation of digital security policies and practices is essential, awareness of the entire school community, including students, teachers and parents, is crucial to ensure a safe and ethical educational environment in the online context.
Keywords: Digital citizenship, Awareness, Privacy, Cyber risks, Digital security.

1 Introdução

A segurança digital e a cidadania online nas instituições educacionais são temáticas emergentes que se tornaram essenciais no contexto atual da educação. Com a crescente inserção das tecnologias digitais nas práticas pedagógicas, é fundamental que alunos e educadores compreendam a importância de uma atuação segura e ética no ambiente online. A segurança digital envolve práticas que protejam dados pessoais, garantam a privacidade e promovam um uso responsável da internet, enquanto a cidadania digital trata da formação de indivíduos conscientes de seus direitos e deveres no espaço digital. Ambas as questões têm raízes no avanço tecnológico e na crescente conectividade da sociedade, que trouxe novos desafios e oportunidades, mas também riscos relacionados à segurança e à ética na internet.

Contextualizando essa temática, observa-se que, com a popularização da internet e das tecnologias digitais nas escolas, os alunos estão cada vez mais expostos a uma série de riscos, como cyberbullying, manipulação de dados, e a disseminação de informações falsas (fake news). Esses riscos não só comprometem a integridade dos indivíduos, mas também afetam o ambiente

escolar, criando a necessidade urgente de discutir e implementar políticas de segurança digital adequadas. A integração da cidadania digital no currículo escolar, por exemplo, pode auxiliar no desenvolvimento do pensamento crítico dos alunos, capacitando-os a agir de forma ética e responsável no ambiente digital.

Exemplificando essa necessidade, muitos casos de vazamento de dados pessoais e de exploração indevida de informações já ocorreram em escolas e universidades, evidenciando a fragilidade das infraestruturas digitais e a falta de conscientização dos envolvidos sobre as práticas seguras online. Um exemplo concreto seria o aumento do uso de redes sociais por estudantes, que, em muitos casos, não têm a consciência sobre os riscos de exposição de suas informações pessoais, o que pode levar a consequências como o roubo de identidade ou assédio virtual.

O problema da pesquisa surge da constatação de que, apesar do crescente uso de tecnologias nas escolas, a segurança digital e a cidadania online ainda são temas pouco discutidos, com a maioria dos educadores e alunos não tendo uma compreensão clara de seus direitos e responsabilidades no mundo digital. Como consequência, muitos não sabem como se proteger contra os riscos e como agir de maneira ética e responsável na internet.

Esta pesquisa se justifica pela necessidade de promover uma reflexão crítica sobre a segurança digital nas instituições educacionais, explorando as práticas que podem ser adotadas para garantir um ambiente virtual seguro e ético. Além disso, busca-se analisar como a cidadania digital pode ser integrada de forma eficaz ao currículo escolar, contribuindo para a formação de cidadãos conscientes e preparados para os desafios do mundo digital.

A relevância da pesquisa está na importância de preparar as novas gerações para viver em um mundo digital cada vez mais complexo e repleto de desafios. A formação de uma cultura de segurança digital e cidadania online nas escolas é essencial para a proteção dos dados pessoais dos alunos e para a promoção de comportamentos responsáveis e éticos na internet, prevenindo danos psicológicos, jurídicos e sociais que podem resultar do uso inadequado das tecnologias.

Este trabalho tem como objetivo investigar os fundamentos da segurança digital e cidadania online nas instituições educacionais, identificando os principais desafios e ameaças que surgem nesse contexto. Além disso, busca analisar estratégias para fortalecer a segurança e a cidadania digital nas escolas, promovendo um ambiente educativo mais seguro e responsável.

O percurso metodológico adotado será uma pesquisa bibliográfica de natureza qualitativa, na qual serão analisados artigos acadêmicos, livros e outros materiais relacionados ao tema, buscando compreender as práticas e abordagens mais eficazes no campo da segurança digital e cidadania online nas escolas. A pesquisa se baseará em uma revisão crítica da literatura existente, buscando identificar lacunas no conhecimento e oferecer contribuições para a implementação de políticas mais eficazes.

No percurso teórico, o estudo fundamenta-se em conceitos de cidadania digital, ética online, segurança digital, e teorias educacionais, abordando a importância de integrar esses temas no currículo escolar e no ambiente educativo. O trabalho também utilizará estudos de caso e exemplos de boas práticas para ilustrar como as escolas podem lidar com os desafios e as ameaças digitais.

Este estudo está estruturado em quatro capítulos. O primeiro capítulo apresenta os fundamentos da arquitetura digital da cidadania, abordando os conceitos-chave de segurança digital e cidadania online. O segundo capítulo discute os desafios e as ameaças à segurança digital no ambiente escolar, identificando os principais riscos e as soluções possíveis. O terceiro capítulo oferece estratégias para fortalecer a segurança e a cidadania digital nas escolas, explorando políticas e práticas eficazes. Por fim, o quarto capítulo apresenta as considerações finais, destacando as conclusões da pesquisa e sugestões para futuras pesquisas e ações nas instituições educacionais.

2 Fundamentos da arquitetura digital na cidadania

A Cidadania Digital é um conceito que engloba a prática e os direitos do indivíduo no ambiente digital, incluindo o uso responsável das tecnologias e a interação com o mundo online de maneira ética. O conceito se originou no contexto das mudanças geradas pela revolução digital e sua crescente influência nas relações sociais, econômicas e políticas. De acordo com Hidd e Costa (2023), a cidadania digital é uma extensão das responsabilidades civis e políticas para o mundo digital, fundamentando-se em princípios como ética, respeito à privacidade e segurança.

No contexto educacional, a cidadania digital assume um papel central, visto que os estudantes estão cada vez mais conectados à internet e expostos a suas diversas dinâmicas. Isso envolve, além do simples acesso à tecnologia, uma educação que forme cidadãos críticos, conscientes e responsáveis. Cunha et al. (2024) discutem a importância da formação digital para os estudantes, propondo que ela seja inclusiva e que ofereça ferramentas para a participação ativa

e segura no ambiente virtual, alinhando os valores da cidadania aos do espaço digital.

Exemplificando, em muitas escolas ao redor do mundo, a cidadania digital tem sido integrada ao currículo como forma de promover a responsabilidade online. No Brasil, por exemplo, algumas iniciativas educacionais buscam ensinar aos alunos não apenas como utilizar as tecnologias, mas também como agir de forma ética e segura no ambiente digital. Além disso, a inclusão de temas como a privacidade de dados e a proteção contra abusos online ajuda a formar cidadãos digitais mais informados e preparados para lidar com os desafios do mundo virtual (Santos, 2023).

Os direitos e responsabilidades no mundo digital estão intimamente ligados à garantia de um uso ético e responsável das tecnologias. Estes direitos incluem a proteção da privacidade, a liberdade de expressão, o direito ao acesso à informação e a proteção contra abusos como cyberbullying e discriminação online. A origem dessa abordagem remonta às discussões sobre a evolução da internet e a necessidade de estabelecer normas que regulem as interações digitais, como proposto pela Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil (Minghelli et al., 2024).

A ética digital surge como um elemento crucial dentro dessa estrutura, pois implica que todos os usuários da internet – sejam eles alunos, professores ou instituições – devem agir com respeito e responsabilidade. Isso envolve não apenas a privacidade de dados, mas também a consideração pelas consequências de ações como a disseminação de informações falsas ou o uso indevido de dados pessoais. A privacidade, por exemplo, é um direito fundamental que

deve ser preservado, tanto pela lei quanto pelas práticas educacionais (Veronese & Rossetto, 2022).

Um exemplo de boas práticas online no ambiente educacional pode ser visto nas iniciativas que buscam garantir que os dados dos alunos sejam protegidos ao utilizar plataformas de ensino. O uso de criptografia de dados e a implementação de senhas fortes são práticas recomendadas. Em algumas escolas, há programas de treinamento que ensinam os alunos a reconhecer riscos como phishing e a agir de forma ética, respeitando os dados de seus colegas e professores, evitando, assim, a violação da privacidade (Lima, 2022).

A Inclusão Digital refere-se ao processo de garantir que todas as pessoas, independentemente de sua classe social, etnia, ou habilidades, tenham acesso às tecnologias da informação e à internet. Esse conceito tem raízes em uma tentativa de combater a exclusão social, proporcionando igualdade de oportunidades no uso das tecnologias. A origem da inclusão digital pode ser traçada às políticas públicas e iniciativas que buscam democratizar o acesso à internet e as ferramentas digitais para todos (Hidd & Costa, 2023).

No ambiente educacional, a inclusão digital é vista como fundamental para que todos os estudantes, especialmente aqueles de classes sociais mais baixas ou com deficiências, possam ter acesso a recursos educacionais digitais. No entanto, ainda existem diversos desafios, como a falta de infraestrutura, o custo elevado dos dispositivos tecnológicos e a necessidade de adaptação das plataformas digitais para garantir a acessibilidade a todos. A inclusão digital, portanto, envolve não apenas o acesso a ferramentas, mas

também a adaptação do conteúdo e das metodologias de ensino para os diferentes públicos (Minghelli et al., 2024).

Exemplos de iniciativas de inclusão digital incluem programas governamentais que fornecem dispositivos gratuitos ou de baixo custo para estudantes, além de escolas que oferecem treinamento especializado para alunos com deficiência. Um exemplo prático é a utilização de softwares de leitura de tela para alunos com deficiência visual, permitindo que eles acessem os mesmos conteúdos que os demais estudantes. Além disso, a criação de conteúdos adaptados, como vídeos com legendas e plataformas com recursos de acessibilidade, é uma prática comum em instituições que buscam garantir a participação equitativa (Santos, 2023).

A Alfabetização Midiática e Informacional envolve a capacidade de identificar, avaliar e analisar criticamente os conteúdos midiáticos e informacionais a que as pessoas são expostas, especialmente na internet. A origem dessa alfabetização está ligada ao crescente volume de informações disponíveis online e à necessidade de educar os indivíduos para que possam discernir o que é verdadeiro ou falso, útil ou irrelevante. A educação midiática visa, assim, equipar os cidadãos com as habilidades necessárias para navegar de maneira crítica e ética pelo vasto universo de informações (Cunha et al., 2024).

Na educação, a alfabetização midiática se tornou uma prioridade, pois as crianças e jovens estão frequentemente expostos a uma grande quantidade de informações, muitas vezes sem a devida orientação para avaliá-las criticamente. Este desafio se torna ainda mais complexo com a disseminação de fake news e desinformação, o que torna crucial que as escolas promovam a reflexão crítica sobre

o conteúdo acessado. A alfabetização midiática, portanto, envolve ensinar os alunos a questionar as fontes, verificar a veracidade dos fatos e compreender a intenção por trás da informação que consomem (Lima, 2022).

Um exemplo de como a alfabetização midiática é aplicada nas escolas é a inclusão de atividades que envolvem a análise de notícias falsas, em que os estudantes são desafiados a investigar a origem de uma informação, comparar diferentes fontes e refletir sobre a ética da disseminação de conteúdos. Além disso, programas educacionais têm sido desenvolvidos para ensinar os alunos a usar as mídias sociais de forma responsável e crítica, promovendo o desenvolvimento de uma postura cidadã digital (Veronese & Rossetto, 2022).

A Cultura Digital refere-se ao uso de ferramentas e tecnologias digitais como parte integrante do cotidiano escolar, promovendo a criação de um ambiente educacional que valorize as interações online de forma segura e ética. Integrar a cidadania digital ao currículo escolar envolve não apenas o uso de dispositivos tecnológicos, mas também a promoção de uma postura crítica e responsável em relação ao ambiente digital. Isso significa ensinar aos alunos sobre a importância da privacidade, segurança, ética e cidadania no mundo online (Santos, 2023).

As escolas desempenham um papel essencial na construção de uma cultura digital sólida, criando espaços de aprendizado onde os alunos possam desenvolver habilidades tecnológicas enquanto compreendem o impacto de suas ações no ambiente virtual. Para isso, é fundamental que as instituições adaptem seus currículos para incluir temas relacionados à segurança digital, ética online e

comportamento responsável nas redes sociais. Além disso, a cultura digital nas escolas deve envolver toda a comunidade escolar – desde os alunos até os educadores e pais – em um esforço conjunto para promover um uso saudável e consciente da tecnologia (Cunha et al., 2024).

Exemplos de integração da cultura digital incluem a criação de oficinas e cursos sobre segurança na internet, o desenvolvimento de projetos que envolvam a criação de conteúdos digitais de forma ética e a realização de debates sobre as consequências de atitudes como o cyberbullying e a disseminação de fake news. A implementação de aulas de cidadania digital no currículo, com discussões sobre ética e direitos digitais, também é uma prática cada vez mais comum em escolas ao redor do mundo (Minghelli et al., 2024).

A Identidade Digital refere-se à forma como os indivíduos se apresentam e são percebidos no ambiente online. No contexto educacional, a construção da identidade digital envolve tanto os alunos quanto os professores, que moldam suas presenças digitais através das interações nas redes sociais, plataformas educacionais e outros meios digitais. A importância de educar os alunos para a construção de uma identidade digital saudável e responsável é fundamental, pois o que é compartilhado online pode ter impactos duradouros em sua vida pessoal, profissional e acadêmica (Hidd & Costa, 2023).

O processo de construção de uma identidade digital requer que os alunos compreendam a diferença entre suas personas online e offline, além de reconhecerem os riscos associados à exposição excessiva nas redes sociais e à divulgação de informações pessoais.

Para isso, as escolas devem proporcionar um ambiente educacional que ensine os estudantes a gerenciar suas presenças digitais de forma cuidadosa e ética. Isso inclui a utilização de ferramentas como configurações de privacidade, gerenciamento de contas online e consciência sobre a impressão digital deixada na internet (Santos, 2023).

Exemplos de como a construção da identidade digital pode ser integrada no currículo escolar incluem atividades que incentivem os alunos a refletirem sobre sua imagem online, tais como a análise de suas interações nas redes sociais ou a criação de projetos digitais que promovam o respeito à privacidade e à autenticidade online. Além disso, ao ensinar sobre a importância de uma presença digital positiva, as escolas contribuem para a formação de indivíduos mais conscientes dos impactos de suas ações na construção de sua identidade (Lima, 2022).

As Fake News e o conceito de Pós-Verdade estão diretamente ligados à disseminação de informações falsas ou manipuladas com o intuito de influenciar opiniões e decisões. O termo "pós-verdade" descreve um cenário onde as emoções e crenças pessoais têm mais influência na formação da opinião pública do que os fatos objetivos. Esse fenômeno é especialmente problemático no ambiente escolar, pois pode afetar o aprendizado dos alunos e sua capacidade de discernir entre o que é verdade e o que é manipulado, impactando negativamente o desenvolvimento do pensamento crítico e da cidadania digital (Cunha et al., 2024).

No contexto educacional, combater as fake news e promover a conscientização sobre a pós-verdade é uma tarefa crucial. As escolas precisam proporcionar aos alunos ferramentas para que eles

possam identificar, questionar e verificar a veracidade das informações que circulam na internet. A alfabetização midiática, abordada anteriormente, desempenha um papel vital nesse processo, ajudando os alunos a desenvolver habilidades críticas para avaliar a confiabilidade de fontes e conteúdos digitais (Hidd & Costa, 2023).

Exemplos de como as escolas podem combater as fake news incluem a realização de debates sobre a natureza da informação, o uso de fontes confiáveis para pesquisas acadêmicas e a implementação de projetos que ensinem os alunos a verificar informações online por meio de ferramentas e práticas como fact-checking. Além disso, programas de conscientização sobre a influência das fake news nas sociedades atuais podem ser implementados, estimulando os alunos a refletirem sobre o impacto da desinformação em suas vidas e na sociedade como um todo (Veronese & Rossetto, 2022).

O Direito ao Esquecimento refere-se à capacidade de um indivíduo de solicitar a remoção de informações pessoais na internet que possam prejudicar sua reputação ou privacidade. Esse conceito tem ganhado relevância no contexto digital devido à persistência de informações online, que podem impactar negativamente a vida pessoal e profissional de indivíduos, incluindo alunos e professores. No ambiente educacional, o direito à privacidade online e a proteção dos dados pessoais são essenciais para garantir um uso seguro e ético da tecnologia (Lima, 2022).

As escolas devem estar cientes da importância de proteger os dados dos alunos e educadores, respeitando os direitos à privacidade e ao esquecimento digital. Isso envolve a implementação de políticas

claras sobre o uso de informações pessoais, garantindo que os dados coletados sejam tratados de forma segura e ética. A implementação da Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil tem sido uma medida importante para regular a coleta e o uso de dados no ambiente escolar, mas ainda existem muitos desafios na aplicação prática dessas diretrizes (Santos, 2023).

Exemplos de como as escolas podem lidar com o direito ao esquecimento e a privacidade incluem a criação de políticas de privacidade claras e acessíveis aos alunos e pais, além de programas educativos que ensinam sobre a importância da proteção de dados pessoais e como garantir a privacidade online. Além disso, escolas devem promover a conscientização sobre o impacto das informações pessoais disponíveis na internet e como elas podem afetar a vida dos indivíduos, criando uma cultura de respeito à privacidade digital (Veronese & Rossetto, 2022).

A internet oferece uma plataforma única para a interação e participação democrática, permitindo que indivíduos se conectem, expressem suas opiniões e se envolvam em discussões sobre questões sociais, políticas e culturais. No contexto escolar, a utilização das redes sociais pode ser uma ferramenta poderosa para incentivar o engajamento dos estudantes em debates e ações coletivas, promovendo uma maior conscientização e responsabilidade cívica. No entanto, essa participação também apresenta desafios relacionados à ética, privacidade e segurança, que precisam ser abordados adequadamente para garantir um ambiente seguro e produtivo (Lima, 2022).

A participação democrática online permite que os alunos desenvolvam habilidades de comunicação, pensamento crítico e

colaboração, essenciais para o exercício da cidadania. A utilização das redes sociais no ambiente escolar deve ser orientada para promover o respeito mútuo, a troca construtiva de ideias e a capacidade de lidar com a diversidade de opiniões. Além disso, as escolas têm a responsabilidade de educar os alunos sobre o impacto de suas palavras e ações nas plataformas digitais, enfatizando a importância da empatia, da educação política digital e da participação cívica consciente (Cunha et al., 2024).

Exemplos de estratégias para promover a interação e a participação democrática na internet nas escolas incluem a organização de fóruns de discussão online sobre temas relevantes para a comunidade escolar, a criação de blogs ou páginas nas redes sociais para promover projetos estudantis e a realização de atividades em que os alunos possam se engajar em ações sociais ou políticas através das plataformas digitais. Além disso, é fundamental incentivar o uso das redes sociais para o debate construtivo e para a construção de uma cultura de respeito à diversidade e à opinião do outro (Veronese & Rossetto, 2022).

3 Desafios e ameaças na segurança digital escolar

O cyberbullying, ou bullying virtual, é um dos maiores desafios enfrentados nas escolas em um ambiente digital. Ele envolve o uso da internet, redes sociais e plataformas digitais para intimidar, humilhar ou assediar indivíduos, frequentemente afetando alunos em idades vulneráveis. A identificação precoce e a intervenção são essenciais para prevenir que o cyberbullying tenha impactos negativos duradouros na saúde mental dos estudantes. As escolas precisam adotar políticas claras para combater esse tipo de

comportamento e promover a cultura de respeito no ambiente virtual (Santos, 2023).

Para combater o cyberbullying, é necessário educar os alunos sobre o que caracteriza essa prática, como reconhecer sinais de assédio e como reagir de maneira responsável. Além disso, as escolas devem criar canais de denúncia seguros, onde os alunos possam relatar incidentes sem medo de retaliação. O trabalho conjunto entre alunos, professores e pais é fundamental para criar um ambiente seguro e de apoio, tanto presencialmente quanto online (Cunha et al., 2024).

Exemplos de ações preventivas incluem a realização de campanhas de conscientização sobre os perigos do cyberbullying, a implementação de programas de apoio psicológico para vítimas e a criação de atividades que promovam a empatia e o respeito no uso das tecnologias. Adicionalmente, as escolas podem oferecer treinamentos para professores e funcionários sobre como lidar com casos de cyberbullying e como criar um ambiente digital positivo e seguro (Lima, 2022).

A exposição de dados pessoais online é uma questão crítica no contexto escolar, já que muitos alunos, professores e até mesmo escolas utilizam plataformas educacionais que coletam e armazenam informações sensíveis. O uso inadequado ou a falta de medidas de segurança podem resultar em vazamento de dados e colocar em risco a privacidade dos indivíduos. As escolas precisam adotar protocolos rigorosos para garantir que os dados dos alunos estejam protegidos, respeitando as legislações de privacidade, como a Lei Geral de Proteção de Dados (LGPD) no Brasil, e educando os

alunos sobre a importância de proteger suas informações pessoais (Santos, 2023).

Além de adotar boas práticas de segurança, é fundamental que os alunos compreendam a relevância de manter suas informações pessoais protegidas. Eles devem ser orientados sobre os riscos de compartilhar dados sensíveis online, como números de telefone, endereços e senhas, e como configurar adequadamente a privacidade em suas contas e dispositivos. As escolas devem promover essa educação digital e desenvolver políticas internas que garantam a segurança da informação no ambiente escolar (Veronese & Rossetto, 2022).

Exemplos de ações que as escolas podem implementar para proteger os dados incluem a escolha de plataformas educacionais que possuam recursos de segurança robustos, a realização de treinamentos sobre proteção de dados e privacidade para alunos e educadores e o uso de sistemas de autenticação e criptografia para proteger as informações armazenadas (Cunha et al., 2024).

Phishing e engenharia social são técnicas de manipulação utilizadas por cibercriminosos para enganar pessoas e obter informações sensíveis, como senhas, números de cartão de crédito e dados pessoais. No contexto educacional, essas práticas podem abranger tanto alunos quanto professores, colocando em risco a segurança de dados escolares e pessoais. O phishing, por exemplo, muitas vezes se apresenta por meio de e-mails falsos, mensagens de texto ou sites fraudulentos que se disfarçam como comunicações legítimas. A engenharia social envolve manipulações psicológicas, onde a vítima é causada a revelar informações proporcionais. A compreensão e a

capacidade de identificar esses ataques são essenciais para evitar danos (Minghelli et al., 2024).

Para prevenir ataques de phishing e engenharia social, as escolas devem promover uma educação digital preventiva. Isso inclui ensinar alunos e educadores a reconhecer sinais de fraudes online, como links suspeitos, erros de digitação em e-mails e o uso de linguagem urgente para solicitar informações. Além disso, as instituições devem adotar políticas de segurança digital, como autenticação de dois fatores, e garantir que todos os membros da comunidade escolar estejam informados sobre os riscos desses ataques. A conscientização contínua é fundamental para fortalecer a defesa contra essas ameaças (Santos, 2023).

Exemplos de medidas para prevenir ataques de phishing incluem a realização de treinamentos e workshops sobre como identificar e-mails e sites fraudulentos. As escolas criam simulações de ataques de phishing como forma de prática podem para alunos e professores, permitindo que eles aprendam a reagir corretamente quando confrontados com tais tentativas. Outro exemplo é a implementação de ferramentas de filtragem de conteúdo para bloquear e-mails e sites suspeitos antes que cheguem aos usuários (Lima, 2022).

O deepfake é uma tecnologia de manipulação digital que utiliza inteligência artificial para criar vídeos ou áudios falsificados, gerando conteúdos altamente convincentes que podem ser usados para espalhar desinformação. Essa técnica tem crescido significativamente e representa um grande desafio para a veracidade da informação, especialmente em um ambiente educacional. No contexto escolar, vídeos e áudios falsificados podem

ser usados para enganar alunos, professores ou até a comunidade escolar, criando um ambiente de desinformação (Hidd & Costa, 2023).

A disseminação de deepfakes nas escolas pode afetar a confiança entre os membros da comunidade escolar e prejudicar a aprendizagem, já que informações falsas podem se espalhar rapidamente nas redes sociais. Além disso, pode gerar situações de bullying ou conflitos, principalmente quando os deepfakes envolvem falsificação de imagens e declarações de indivíduos, como alunos ou professores. A educação digital, focada em desenvolver a capacidade crítica dos alunos, é essencial para evitar que tais conteúdos aceitos sejam sem seleção (Cunha et al., 2024).

Exemplos de estratégias para combater o uso de deepfakes nas escolas incluem a implementação de programas de alfabetização digital que fazem com que os alunos verifiquem a veracidade das informações antes de serem fornecidas. As escolas podem criar parcerias com especialistas em tecnologia para detectar deepfakes e garantir que as informações divulgadas dentro da comunidade escolar sejam precisas. Também é importante promover a utilização de ferramentas de verificação de conteúdo, como softwares de detecção de manipulação digital, para ajudar os alunos a identificar conteúdos falsificados (Veronese & Rossetto, 2022).

As plataformas de ensino, que se tornaram indispensáveis no contexto educacional contemporâneo, podem apresentar riscos relacionados ao vazamento de dados pessoais dos usuários. Esses sistemas armazenam frequentemente informações sensíveis sobre alunos e professores, como nomes, endereços, registros acadêmicos e consultas. Caso as medidas de segurança não sejam especificadas,

os dados privados podem ser acessados e utilizados de maneira indevida. A das plataformas educacionais é, portanto, um aspecto fundamental para proteger a segurança dos usuários e garantir a integridade da educação digital (Minghelli et al., 2024).

O uso de plataformas de ensino requer atenção especial em relação ao gerenciamento de dados e à implementação de práticas adequadas de segurança cibernética. Além disso, as escolas devem garantir que os fornecedores de plataformas digitais sigam rigorosamente as regulamentações de proteção de dados, como a LGPD, para garantir que os dados dos alunos sejam protegidos. A conscientização sobre os riscos e as boas práticas de uso dessas plataformas deve ser um componente essencial da formação digital de alunos e professores (Santos, 2023).

Exemplos de medidas para garantir a segurança nas plataformas de ensino incluem a implementação de auditorias regulares nas ferramentas digitais utilizadas pela escola, a implementação de autenticação multifatorial para acessos às plataformas e a educação dos alunos sobre como gerenciar suas informações pessoais online. As escolas também realizam testes de segurança e investem em tecnologias de criptografia para proteger os dados seguros armazenados nessas plataformas (Lima, 2022).

O uso de inteligência artificial (IA) na educação tem o potencial de transformar a forma como os alunos aprendem e interagem com os conteúdos. No entanto, o seu uso indevido pode gerar sérios problemas éticos, como a invasão de privacidade e a discriminação algorítmica. A IA pode ser usada para personalizar o aprendizado, mas também pode ser usada para monitoramento excessivo dos alunos, criando uma sensação de vigilância constante. A ética do uso

da IA na educação deve ser discutida para garantir que a tecnologia seja aplicada de maneira justa e sem prejudicar os direitos dos alunos (Cunha et al., 2024).

No ambiente educacional, a IA pode ser empregada de diversas formas, como sistemas de recomendação de conteúdos, análise de desempenho acadêmico e até mesmo avaliação automática. No entanto, é crucial que essas tecnologias sejam utilizadas com responsabilidade e transparência. O uso de IA para monitorar comportamentos dos alunos ou avaliar suas emoções sem o devido consentimento pode ser problemático. Portanto, a regulamentação e a ética são questões centrais para garantir que a IA no contexto educacional não viole os direitos fundamentais dos indivíduos (Hidd & Costa, 2023).

Exemplos de boas práticas no uso da IA na educação incluem a criação de diretrizes claras sobre a coleta e o uso de dados dos alunos, garantindo que as ferramentas de IA sejam transparentes quanto ao funcionamento dos algoritmos. Além disso, é fundamental que os educadores sejam treinados para entender os limites e as implicações éticas do uso da IA em sala de aula. As escolas também devem estar preparadas para proteger os dados pessoais dos alunos contra possíveis abusos ou exploração (Veronese & Rossetto, 2022).

A superexposição digital é uma preocupação crescente, especialmente entre os jovens, que podem passar longas horas em frente às telas, seja para fins educacionais ou recreativos. O uso excessivo de dispositivos digitais pode levar a uma série de problemas psicológicos, como ansiedade, depressão e dependência tecnológica. Esses problemas podem afetar o desempenho

acadêmico dos alunos e comprometer sua saúde mental, criando um ciclo de dependência que dificulta o equilíbrio entre o ambiente digital e o real (Santos, 2023).

O ambiente digital oferece uma série de estímulos que podem ser altamente viciantes, como redes sociais, jogos online e conteúdo multimídia. Esses estímulos podem levar os alunos a priorizar o ritmo de tela em detrimento de atividades mais saudáveis, como interações sociais face a face e práticas físicas. A falta de equilíbrio pode causar isolamento social e emocional, afetando a autoestima e o bem-estar mental. Portanto, a educação digital deve incorporar estratégias para promover o uso consciente das tecnologias e evitar a superexposição (Cunha et al., 2024).

Exemplos de estratégias para reduzir os impactos psicológicos da superexposição digital incluem a implementação de programas de conscientização sobre os riscos do uso excessivo da tecnologia, além de práticas como a educação socioemocional para ensinar os alunos a lidar com o estresse e a ansiedade digital. As escolas estabelecem limites de tempo para o uso de dispositivos eletrônicos em atividades escolares e podem promover a prática de atividades offline, como esportes e encontros sociais. Isso pode ajudar a garantir que os alunos desenvolvam uma relação saudável com a tecnologia (Minghelli et al., 2024).

A dark web é uma parte da internet que não é indexada por motores de busca comuns e onde ocorrem atividades ilícitas, como o comércio de drogas, armas e dados roubados. Embora a maioria dos usuários da internet não tenha contato com a dark web, o acesso a conteúdos perigosos é um risco crescente, especialmente para os jovens, que podem ser atraídos por essa parte obscura da rede. A

conscientização sobre os perigos da dark web e a promoção de comportamentos seguros online são essenciais para proteger os alunos desses riscos (Veronese & Rossetto, 2022).

No contexto educacional, é fundamental que as escolas adotem uma abordagem de conscientização sobre os perigos da dark web e do acesso a conteúdos ilegais. Isso envolve ensinar aos alunos sobre as consequências legais e os riscos à sua segurança ao acessar sites da dark web. Além disso, as escolas devem implementar programas de prevenção que abordem temas como crimes cibernéticos, segurança online e como atividades sérias suspeitas na internet. Isso pode ajudar a proteger os alunos de se envolverem em comportamentos perigosos ou criminosos online (Lima, 2022).

Exemplos de práticas preventivas incluem o desenvolvimento de campanhas de conscientização nas escolas, que explicam o que é uma dark web, como ela funciona e os perigos envolvidos. As escolas também podem usar filtros de conteúdo em redes de Wi-Fi para bloquear o acesso a sites ilegais, além de promover workshops e palestras com especialistas em segurança cibernética. Além disso, é importante que os alunos aprendam como buscar ajuda caso se deparem com conteúdo perigoso ou atividades suspeitas online (Santos, 2023).

As regulamentações sobre segurança digital são essenciais para proteger os dados pessoais e garantir a privacidade dos indivíduos em um ambiente cada vez mais digitalizado. A Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil e o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia são legislações que têm como objetivo garantir a proteção da privacidade e a segurança dos dados pessoais dos usuários online. Essas leis estabelecem

diretrizes claras sobre como os dados devem ser coletados, processados e armazenados, além de exigir o consentimento dos indivíduos para o uso de suas informações (Cunha et al., 2024).

No contexto educacional, a LGPD e o GDPR têm implicações diretas, já que escolas e universidades lidam com dados sensíveis de alunos e professores. Isso inclui dados acadêmicos, informações de saúde e outros dados pessoais que precisam ser protegidos contra vazamentos ou usos indevidos. As instituições de ensino devem garantir que suas plataformas digitais e sistemas de gestão de dados estejam em conformidade com essas regulamentações, adotando medidas de segurança cumpridas e garantindo o consentimento informado dos usuários (Hidd & Costa, 2023).

Exemplos de boas práticas para garantir a conformidade com a LGPD e o GDPR incluem a implementação de políticas internas de privacidade, a realização de auditorias regulares sobre o uso de dados e a capacitação de funcionários e alunos sobre como proteger suas informações pessoais. As escolas também devem estabelecer procedimentos claros para o uso de dados sensíveis e garantir que os sistemas usados para armazenar essas informações sejam seguros e confiáveis. Além disso, é importante que as escolas tenham uma responsabilidade pela proteção de dados, conforme exigido pela LGPD e GDPR (Minghelli et al., 2024).

4 Considerações Finais

O objetivo geral deste trabalho foi investigar os fundamentos da segurança digital e cidadania online nas instituições educacionais, identificando os principais desafios e ameaças, e explorando estratégias para fortalecer esses aspectos nas escolas. Esse objetivo

foi alcançado, pois conseguimos analisar, de forma detalhada, as questões relacionadas à segurança digital e à cidadania online no contexto educacional, abordando tanto os riscos quanto as soluções para criar um ambiente virtual mais seguro e ético. A pesquisa contribuiu para a compreensão das práticas e abordagens para proteger dados pessoais e promover um uso responsável das tecnologias.

Os principais resultados desta pesquisa incluem a identificação dos maiores desafios enfrentados pelas escolas em relação à segurança digital, como cyberbullying, exposição de dados pessoais, e disseminação de notícias falsas. Além disso, foram destacadas as boas práticas que podem ser adotadas nas instituições educacionais para promover a cidadania digital, como a integração desses temas no currículo escolar, a criação de políticas de segurança digital e a capacitação de alunos, professores e famílias. A pesquisa também evidenciou a necessidade urgente de um maior envolvimento da comunidade escolar na construção de uma cultura digital, ética e responsável.

A pesquisa oferece importantes contribuições teóricas ao integrar o conceito de cidadania digital com o contexto educacional, mostrando como as escolas podem desempenhar um papel crucial na formação de cidadãos digitais conscientes e responsáveis. Além disso, a reflexão sobre as ameaças digitais e as estratégias de segurança propôs uma abordagem integrada e multidisciplinar, unindo elementos de ética, educação e tecnologia. Isso enriqueceu o entendimento de como esses temas podem ser envolvidos de maneira prática nas escolas.

A pesquisa não encontrou limitações significativas em relação aos métodos adotados. Uma metodologia de pesquisa bibliográfica qualitativa foi eficaz para o alcance dos objetivos propostos, permitindo uma análise abrangente e crítica da literatura existente sobre o tema. Não foram observadas restrições na coleta de dados, uma vez que o estudo se baseou em fontes acadêmicas e documentais que forneceram uma base sólida para as conclusões. O estudo foi conduzido de maneira ampla, abrangendo uma variedade de perspectivas e práticas relacionadas à segurança digital e à cidadania online.

Embora a pesquisa tenha sido abrangente, sugere-se que futuros estudos realizem investigações mais práticas, como estudos de caso em escolas específicas, para analisar como as políticas de segurança digital e cidadania online são renovadas no dia a dia escolar. Também é importante explorar a eficácia de programas de conscientização em diferentes faixas etárias e contextos culturais, além de avaliar o impacto das tecnologias emergentes, como a inteligência artificial, nas questões de segurança digital e ética online nas escolas.

REFERÊNCIAS BIBLIOGRÁFICAS

Cunha, C. R., Albuquerque, M. A. B. de ., & Silva, K. C. V. da . Lei Geral de Proteção de Dados Pessoais e a relevância de sua implantação. **Revista Do Instituto De Direito Constitucional E Cidadania**, 8(1), e078. https://doi.org/10.48159/revistadoidcc.v8n1.e078. 2024.

Hidd, C. de C. L., & Costa, P. M. da., S. Proteção dos dados pessoais na realidade virtual:: ponderações sobre o Meta® na égide do

Constitucionalismo Digital. **Revista Eletrônica Direito & TI**, 1(15), 81–107. Recuperado de https://direitoeti.emnuvens.com.br/direitoeti/article/view/127. 2023.

Lima, C. M. de. **Avaliação de riscos cibernéticos aplicado ao processo de consciência situacional do Centro de Defesa Cibernética do Comando da Aeronáutica.** 2022. xvi, 199 f., il. Dissertação (Mestrado Profissional em Computação Aplicada) — Universidade de Brasília, Brasília. 2022.

Minghelli, M., Garcia B. B., Vale, M. A do., Santos P. S. Lei Geral de Proteção de Dados e a elaboração do Relatório de Impacto à Proteção de Dados Pessoais. **Em Quest.** Available from: https://doi.org/10.1590/1808-5245.30.138249. 2024.

Santos, M. R. de J. **Análise da proteção dos dados de alunos nas escolas públicas de Valença: uma abordagem de cibersegurança.** 2023. Trabalho de Conclusão de Curso (Tecnólogo em ADS) - Instituto Federal de Educação, Ciência e Tecnologia da Bahia, Valença. 2023.

Veronese, J. R. P., & Rossetto, G. M. de F.. O quadrilema da exclusão, inclusão, superexplorações e proteção de dados pessoais de crianças e adolescentes na perspectiva da fraternidade. **Sequência (florianópolis)**, 43(92), e92875. https://doi.org/10.5007/2177-7055.2022.e92875. 2022.

---

[1] Mestranda em Tecnologias Emergentes da Educação pela Must University. E-mail: acesse o artigo original para visualizar o e-mail.

[2] Coordenador pedagógico da prefeitura municipal de Picos-PI. Mestre em Tecnologias Emergentes da Educação pela Must University. E-mail: acesse o artigo original para visualizar o e-mail.