REVISTA TÓPICOS

PRERROGATIVAS E ÓBICES DA CIDADÂNIA ONLINE: UM OLHAR SOBRE A SEGURANÇA DIGITAL NAS INSTITUIÇÕES EDUCACIONAIS

DOI: 10.5281/zenodo.14807869

Juliane Aparecida Pereira Borges[1]
Anna Júlia Borges de Moraes[2]
Micael Campos da Silva[3]
Kevin Cristian Paulino Freires[4]

RESUMO

Esta pesquisa aborda a importância crescente da cidadania digital no contexto educacional, especialmente no que diz respeito à segurança online e à proteção de dados pessoais. Desse modo, com o avanço das tecnologias digitais e a digitalização dos processos educacionais, surgem desafios relacionados à privacidade e à segurança da informação nas escolas, o que torna necessário discutir as prerrogativas e responsabilidades digitais dos envolvidos no ambiente escolar. Nessa perspectiva, a pesquisa objetiva analisar os obstáculos e as prerrogativas da cidadania online nas instituições educacionais, com foco nas questões de privacidade e segurança digital, propondo estratégias para o fortalecimento da segurança nas escolas. À vista disso, a pesquisa foi conduzida por meio de uma metodologia bibliográfica, de natureza qualitativa. Sendo assim, o objetivo

da pesquisa foi alcançado, uma vez que foram identificados os principais obstáculos e soluções para melhorar a segurança digital nas escolas. Assim, a pesquisa contribui teoricamente para investigar a relação entre a cidadania digital e a proteção de dados no contexto educacional, propondo uma abordagem integrada sobre a segurança digital nas instituições de ensino. Ainda assim, as limitações do estudo foram mínimas, dado o caráter qualitativo da pesquisa, mas sugerem a necessidade de investigações empíricas para complementar a análise teórica. Logo, futuros trabalhos podem aprofundar a implementação de políticas práticas de segurança digital nas escolas e avaliar a eficácia das capacitações específicas para educadores e gestores escolares.
Palavras-chave: Cidadania digital, Conscientização, Privacidade, Riscos cibernéticos, Segurança digital.

ABSTRACT

This research addresses the growing importance of digital citizenship in the educational context, especially with regard to online security and the protection of personal data. Therefore, with the advancement of digital technologies and the digitalization of educational processes, challenges arise related to privacy and information security in schools, which makes it necessary to discuss the digital prerogatives and responsibilities of those involved in the school environment. From this perspective, the research aims to analyze the obstacles and prerogatives of online citizenship in educational institutions, focusing on issues of privacy and digital security, proposing strategies to strengthen security in schools. In view of this, the research was conducted using a bibliographic methodology, of a qualitative

nature. Therefore, the objective of the research was achieved, as the main obstacles and solutions to improving digital security in schools were identified. Thus, the research theoretically contributes to investigating the relationship between digital citizenship and data protection in the educational context, proposing an integrated approach to digital security in educational institutions. Even so, the limitations of the study were minimal, given the qualitative nature of the research, but they suggest the need for empirical investigations to complement the theoretical analysis. Therefore, future work can deepen the implementation of practical digital security policies in schools and evaluate the effectiveness of specific training for educators and school managers.
Keywords: Digital citizenship, Awareness, Privacy, Cyber risks, Digital security.

1 Introdução

A cidadania online é um conceito que surgiu com o avanço das tecnologias digitais e a presença crescente da internet no cotidiano das pessoas. Dessa forma, a noção de ser cidadão no mundo virtual implica não apenas o uso de plataformas digitais, mas também o entendimento das prerrogativas e responsabilidades associadas ao comportamento online. Nessa perspectiva, a origem desse conceito remonta ao momento em que a internet passou a ser um espaço de interação social, educativo e até político, criando a necessidade de uma cidadania digital que oferecesse direitos e deveres aos usuários. Este conceito tem relevância com o aumento da digitalização das instituições educacionais, o que inclui desde o uso de plataformas para

ensino até o compartilhamento de dados sensíveis de alunos e educadores. Em face disso, surgem questões sobre as prerrogativas e os obstáculos à cidadania online, com destaque para a segurança digital nas escolas.

Dessa maneira, o contexto da cidadania online nas instituições educacionais está diretamente ligado à dependência crescente de tecnologias digitais, tanto para atividades pedagógicas quanto administrativas. Nesse viés, a escola, como instituição que visa o desenvolvimento integral do ser humano, precisa se adaptar a essa realidade, garantindo que seus alunos, educadores e demais envolvidos possam atuar no ambiente digital com segurança. Exemplificando, a utilização de ferramentas como plataformas de ensino a distância, redes sociais educacionais e armazenamento de informações sensíveis exige uma abordagem cuidadosa sobre como proteger dados pessoais e garantir que a privacidade e a integridade dos envolvidos sejam respeitadas.

Diante disso, o problema desta pesquisa reside na lacuna existente entre as prerrogativas de uma cidadania digital segura e as dificuldades práticas enfrentadas pelas instituições educacionais para implementar medidas efetivas de segurança online. Apesar da crescente conscientização sobre a importância da segurança digital, ainda são comuns falhas na proteção de dados e na exposição de informações sensíveis, colocando em risco a privacidade de alunos e educadores. Além disso, a falta de treinamento adequado e a resistência às mudanças tecnológicas nas escolas agravaram o problema, tornando fundamental o estudo sobre as responsabilidades digitais no contexto educacional.

Além do mais, a justificativa da pesquisa baseia-se na necessidade de promover uma compreensão maior das questões de segurança digital no ambiente escolar. Esta pesquisa se justifica pela urgência em discutir a proteção de dados pessoais e a privacidade no contexto educacional, de forma a garantir que a cidadania digital seja exercida de maneira responsável e segura. Dada a exposição crescente das instituições educacionais a ameaças cibernéticas, é fundamental explorar as estratégias que podem ser adotadas para mitigar riscos e promover a educação sobre segurança digital.

Ainda assim, a relevância da pesquisa é evidente, uma vez que a proteção de dados e a segurança online são temas cruciais para o desenvolvimento da cidadania digital responsável, especialmente no ambiente escolar. Assim sendo, a educação para a segurança digital apresenta-se como uma ferramenta essencial para a formação de cidadãos críticos e conscientes sobre suas responsabilidades no ambiente online, promovendo não apenas o uso adequado das tecnologias, mas também o respeito pelos direitos de todos os envolvidos no processo educacional.

Diante do exposto, o objetivo da pesquisa é analisar as prerrogativas e obstáculos à cidadania online nas instituições educacionais, com foco especial nas questões de privacidade e segurança de dados, e propor estratégias de melhoria para o fortalecimento da segurança digital nas escolas. Ademais, a pesquisa busca identificar as principais ameaças cibernéticas enfrentadas pelas instituições educacionais e de orientação

abordagens preventivas, além de investigar as práticas de capacitação continuada para educadores e gestores escolares.

Nesse sentido, o percurso metodológico adotado será uma pesquisa bibliográfica de natureza qualitativa, com o intuito de revisar e analisar as principais teorias e estudos já existentes sobre o tema. Uma abordagem qualitativa permitirá uma análise das práticas educacionais, das políticas de segurança digital e das experiências de instituições que implementaram soluções eficazes.

No que diz respeito ao percurso teórico, a pesquisa será fundamentada em conceitos sobre cidadania digital, privacidade online, segurança da informação e nas particularidades do contexto educacional. A partir dessa base teórica, será possível identificar as relações entre os direitos e responsabilidades digitais e as práticas escolares, propondo soluções que estejam em conformidade com as melhores práticas de segurança e privacidade.

Com isso, este trabalho será estruturado em quatro capítulos principais: 1) Introdução, onde serão apresentados os temas centrais, o problema de pesquisa, a justificativa, a relevância e os objetivos; 2) Prerrogativas e responsabilidades digitais no ambiente escolar, com ênfase na privacidade e segurança de dados pessoais; 3) Ameaças cibernéticas e segurança institucional, abordando estratégias preventivas e a importância da capacitação contínua dos profissionais da educação; 4) Considerações finais, onde serão considerados os resultados da pesquisa e as possíveis opções para futuras ações no campo da segurança digital educacional.

2 Prerrogativas e responsabilidades digitais no ambiente escolar: Privacidade e salvaguarda de dados pessoais

Os direitos e deveres dos usuários no ambiente escolar digital referem-se às normas que regem a utilização de ferramentas e recursos digitais nas instituições de ensino. A origem desses direitos remonta aos conceitos de cidadania digital, que emergem com a crescente presença das tecnologias no cotidiano, especialmente a partir da década de 1990, quando a internet se popularizou (Hidd., & Costa, 2023). Estes direitos e devem ser estabelecidos para garantir que os usuários, como alunos, professores e funcionários, utilizem as tecnologias de maneira responsável, respeitando normas de comportamento e privacidade.

No contexto educacional, os direitos dos usuários incluem o direito à privacidade, à segurança de suas informações pessoais e ao acesso igualitário às tecnologias. Já os deveres envolver o compromisso de utilizar as ferramentas digitais de forma ética e responsável, respeitando as regras de conduta e evitando práticas como o cyberbullying, o uso de dados de forma indevida e o plágio (Hidd., & Costa, 2023). Uma instituição educacional deve garantir que esses direitos e devem ser bem compreendidos e aplicados por todos os envolvidos.

Exemplificando, os alunos têm o direito de acessar materiais educacionais on-line sem preocupação com seus dados pessoais vendidos a empresas ou expostos sem consentimento (Hidd., & Costa, 2023). Ao mesmo tempo, eles têm o dever de respeitar os conteúdos protegidos por direitos autorais e de não utilizar as plataformas digitais da escola para fins pessoais ou

específicos (Hidd., & Costa, 2023). Os professores, por sua vez, têm o dever de orientar os alunos sobre a utilização ética da internet e da privacidade digital, garantindo que suas ações on-line sigam as diretrizes da escola (Hidd., & Costa, 2023).

Dessa forma, políticas de privacidade e regras de dados são os conjuntos de normas e diretrizes condicionais para garantir que as informações pessoais dos alunos e colaboradores sejam protegidas no ambiente digital (Lima, 2022). Essas políticas têm sua origem nas leis de proteção de dados, como a Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil, que surgiu como uma resposta à crescente coleta e utilização de dados pessoais sem a obrigação de transparência e consentimento, nos quais as políticas visam o uso, armazenamento e compartilhamento de dados pessoais dentro das instituições educacionais.

Nessa perspectiva, a implementação de políticas de privacidade nas escolas é fundamental para proteger os dados dos estudantes e garantir a conformidade com as leis de proteção de dados (Lima, 2022). Estas políticas devem definir de forma clara como os dados serão coletados, utilizados e armazenados, garantindo que os alunos e suas famílias sejam informados sobre o uso de seus dados e que possam consentir com as práticas impostas. Além disso, devem ser previstas normas de segurança digital, como o uso de senhas fortes e a criptografia de informações confidenciais.

Um exemplo comum de política de privacidade nas escolas é o consentimento expresso dos pais ou responsáveis para o uso de dados das

aulas em plataformas educacionais online (Lima, 2022). Além disso, algumas escolas adotam regras como a anonimização de dados em sistemas de gestão escolar, limitando o acesso de terceiros a informações sensíveis, como notas e dados pessoais. Outra prática comum é o treinamento contínuo de funcionários e educadores para garantir que eles compreendam e sigam as diretrizes de privacidade e proteção de dados (Lima, 2022).

Ainda assim, o manejo seguro de dados pessoais envolve a implementação de práticas e medidas para proteger as informações previstas para alunos e educadores contra vazamentos, acessos não autorizados e outras ameaças, no qual a origem dessa necessidade está diretamente relacionada ao aumento da digitalização de dados e à vulnerabilidade das informações pessoais no ambiente online (Minghelli et al., 2024). Estratégias eficazes para o gerenciamento seguro de dados pessoais surgiram com o fortalecimento das leis de proteção de dados, como o GDPR na União Europeia e a LGPD no Brasil, que estabeleceram a responsabilidade das organizações em proteger dados pessoais.

Nesse sentido, as estratégias para o manejo seguro de dados incluem práticas como o uso de sistemas de segurança cibernética avançada, criptografia de dados sensíveis e políticas rigorosas de acesso à informação. Além disso, as escolas devem investir em treinamento regular para seus funcionários, garantindo que todos saibam como manusear, armazenar e excluir corretamente os dados pessoais dos alunos e educadores (Minghelli et al., 2024). Também é importante realizar

auditorias regulares para garantir que as normas de segurança sejam cumpridas e que as vulnerabilidades sejam rapidamente corrigidas.

Exemplificativamente, algumas escolas utilizam sistemas de gerenciamento de dados educacionais que implementam autenticação multifatorial e criptografia para proteger as informações dos alunos, como notas e histórico escolar (Minghelli et al., 2024). Outras adotam plataformas de ensino com políticas rígidas sobre o uso e armazenamento de dados, garantindo que as informações de login e dados protegidos sejam armazenados de maneira segura e que apenas pessoas autorizadas tenham acesso a esses dados (Minghelli et al., 2024).

3 Ameaças cibernéticas e segurança institucional: Abordagens preventivas e capacitação contínua

As ameaças cibernéticas são ataques ou ações maliciosas praticadas por indivíduos ou grupos com o objetivo de acessar, corromper ou roubar dados seguros. Essas ameaças podem ter várias origens, incluindo hackers, softwares maliciosos, phishing e outros métodos de intrusão (Santos, 2023). As instituições educacionais, devido à grande quantidade de dados pessoais e informações disponíveis que manipulam, são alvos frequentes de tais ameaças. A origem desses ataques está frequentemente associada ao uso crescente de tecnologias digitais nas escolas, que, embora tragam benefícios, também aumentam a superfície de ataque (Santos, 2023).

Desse modo, as ameaças cibernéticas que afetam as escolas podem variar desde ataques de ransomware, que bloqueiam o acesso a sistemas e

bloqueiam resgates, até a coleta ilegal de dados pessoais por meio de phishing, onde os hackers tentam enganar os usuários para que revelem suas credenciais (Santos, 2023). Além disso, as escolas também podem ser alvo de ataques aos seus sistemas de gestão, prejudicando a integridade dos dados dos alunos e professores, no qual a evolução constante das técnicas de ataque torna esses desafios ainda mais complexos, exigindo vigilância constante e medidas de segurança adequadas.

Exemplificando, um caso comum de ameaça cibernética nas escolas é o ataque de ransomware, onde hackers invadem os sistemas de uma instituição educacional e bloqueiam o acesso aos dados até que um resgate seja pago (Santos, 2023). Outro exemplo é o phishing, em que e-mails falsos são enviados para professores e alunos, com links que, ao serem clicados, capturam dados pessoais e credenciais de acesso (Santos, 2023). Além disso, a coleta de dados em plataformas educacionais sem medidas de segurança também pode ser vista como uma ameaça cibernética.

Nesse viés, os protocolos de segurança digital são um conjunto de normas e práticas que visam proteger os sistemas e dados digitais das instituições educacionais contra ataques cibernéticos (Veronese., & Rossetto, 2022). Dessa forma, a origem desses protocolos remonta à necessidade de criar sistemas de defesa robustos para proteger as informações contra a crescente ameaça digital, com base nas melhores práticas de segurança cibernética e nas regulamentações de proteção de dados, como a LGPD e GDPR.

Ademais, os protocolos de segurança digital incluem a implementação de firewalls, criptografia de dados, autenticação multifatorial e o treinamento

constante de todos os envolvidos na gestão de dados (Veronese., & Rossetto, 2022). Além disso, é essencial que as escolas estabeleçam um plano de resposta a incidentes, que oriente as ações a serem tomadas em caso de um ataque cibernético, minimizando os danos e garantindo uma recuperação rápida dos sistemas afetados.

Exemplificativamente, uma escola pode adotar a autenticação multifatorial para garantir que apenas usuários autorizados acessem sistemas com dados sensíveis (Veronese., & Rossetto, 2022). Outra medida de segurança comum é a criptografia de dados, como nas plataformas de ensino, onde as informações dos alunos são armazenadas de forma segura e ilegíveis para qualquer pessoa não autorizada (Veronese., & Rossetto, 2022). Além disso, as instituições podem realizar simulações de ataques para treinar sua equipe sobre como agir em caso de incidentes de segurança.

Sendo assim, programas de capacitação e conscientização são iniciativas que visam educar e treinar os educadores e gestores escolares sobre as melhores práticas de segurança digital e como prevenir ataques cibernéticos (Cunha., Albuquerque., & Silva, 2024). Dessa maneira, a origem desses programas é a necessidade de formar uma cultura de segurança digital dentro das escolas, garantindo que todos os envolvidos compreendam as ameaças e saibam como se proteger, nos quais esses programas surgiram com o aumento das ameaças cibernéticas e a necessidade de treinar os profissionais da educação para lidar com a nova realidade digital.

Com isso, a capacitação de educadores e gestores envolve a oferta de cursos e workshops sobre segurança digital, onde são abordados tópicos como proteção de dados pessoais, criação de senhas fortes, identificação de ataques cibernéticos e prevenção de phishing (Cunha., Albuquerque., & Silva, 2024). Além do mais, é importante que esses programas incluam estratégias de conscientização contínua, mantendo todos os dados informados sobre as últimas ameaças e melhores práticas de segurança, no qual a capacitação deve ser um processo contínuo, dada a rápida evolução das ameaças cibernéticas.

À exemplo disso, muitas escolas adotam programas anuais de treinamento para educadores, abordando temas como privacidade online, proteção contra malware e como identificar e-mails suspeitos (Cunha., Albuquerque., & Silva, 2024). Alguns investidores participam de seminários sobre a implementação de políticas de segurança institucional e a importância de criar uma cultura de segurança dentro da escola (Cunha., Albuquerque., & Silva, 2024). Além disso, os professores podem ser treinados para educar os alunos sobre os riscos da internet e como navegar de forma segura.

4 Considerações Finais

O objetivo desta pesquisa foi analisar as prerrogativas e obstáculos à cidadania online nas instituições educacionais, com foco especial nas questões de privacidade e segurança de dados, propondo estratégias de melhoria para o fortalecimento da segurança digital nas escolas. Este objetivo foi alcançado, uma vez que a pesquisa conseguiu abordar as

principais questões relativas à cidadania digital, destacando as responsabilidades e os desafios enfrentados pelas instituições educacionais na proteção de dados e privacidade de seus membros. Além disso, foram identificadas e discutidas as principais ameaças cibernéticas e as estratégias preventivas que podem ser adotadas para garantir um ambiente digital seguro nas escolas.

Desse modo, os principais resultados desta pesquisa indicam que, apesar de haver uma crescente conscientização sobre a importância da segurança digital nas instituições educacionais, ainda existem lacunas significativas na implementação de medidas de proteção de dados pessoais e capacitação dos educadores para lidar com as questões de segurança digital. Ainda assim, a pesquisa evidenciou também a necessidade de políticas mais robustas e específicas específicas à proteção de dados no ambiente escolar, além de um investimento contínuo em treinamentos para gestores e professores, para que possam enfrentar as ameaças cibernéticas de forma mais eficazes.

Em termos de contribuições teóricas, este trabalho é destacado ao investigar a relação entre cidadania digital e segurança online, em especial no contexto educacional. Além do mais, a pesquisa trouxe à tona a importância de integrar as discussões sobre privacidade e segurança digital ao currículo educacional, apontando uma abordagem mais ampla que não se limita apenas ao uso de ferramentas digitais, mas também ao fortalecimento da educação sobre a segurança da informação. Ainda assim, a construção teórica sobre as prerrogativas e obstáculos da cidadania

online, fundamentada em uma revisão crítica das práticas atuais, abre novas perspectivas para futuras investigações na área.

Quanto às limitações, pode-se afirmar que a pesquisa não apresentou grandes restrições quanto ao seu escopo ou à sua metodologia. Ademais, a abordagem qualitativa e a pesquisa bibliográfica permitiram uma análise do tema, garantindo uma compreensão ampla dos desafios e das soluções no campo da segurança digital nas escolas. No entanto, é importante considerar que os resultados são baseados numa análise teórica, e que uma pesquisa empírica envolvendo entrevistas com gestores e educadores poderia complementar ainda mais as explicações aqui apresentadas.

Com isso, diante dos resultados obtidos e das limitações do estudo, sugiro que futuros trabalhos na área se aprofundem na implementação de políticas práticas de segurança digital nas escolas. Além disso, seria interessante realizar estudos empíricos para avaliar a eficácia das estratégias preventivas propostas, analisando o impacto real das capacitações e das políticas de proteção de dados na prática cotidiana das instituições educacionais. Logo, a pesquisa também poderia explorar a integração de ferramentas de segurança digital com outras áreas do currículo escolar, ampliando o debate sobre cidadania digital e segurança em um contexto mais amplo e interdisciplinar.

REFERÊNCIAS BIBLIOGRÁFICAS

Cunha, C. R., Albuquerque, M. A. B. de ., & Silva, K. C. V. da . (2024). 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.

Hidd, C. de C. L., & Costa, P. M. da., S. (2023). 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.

Lima, C. M. de. (2022). 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.

Minghelli, M., Garcia B. B., Vale, M. A do., Santos P. S. (2024). 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.

Santos, M. R. de J. (2023). 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.

Veronese, J. R. P., & Rossetto, G. M. de F.. (2022). 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.

[1] Mestranda em Tecnologias Emergentes em Educação pela Must University. e-mail: julianeaparecida2012@hotmail.com.

[2] Especialista em Orientação Educacional pela Faculdade Metropolitana do Cariri. e-mail: annajuliamoraes.m@gmail.com.

[3] Coordenador pedagógico da prefeitura municipal de Picos-PI. Mestre em Tecnologias Emergentes da Educação pela Must University. e-mail: micaelcamposdasilva@gmail.com.

[4] Docente de deficiência intelectual e TEA na SEDU. Doutorando em Ciências da Educação pela FAcultad Interamericana de Ciencias Sociales. e-mail: freireskeven43@gmail.com.