REVISTA TÓPICOS

A IMPORTÂNCIA DA SEGURANÇA E DA CIDADANIA DIGITAL NA ERA DA INFORMAÇÃO

DOI: 10.5281/zenodo.16790528

Zulma Nascimento Guidi[1]

RESUMO

O objetivo deste estudo é analisar a importância da segurança e da cidadania digital, destacando os principais desafios enfrentados e as soluções propostas para superá-los. Para alcançar esses objetivos, utilizou-se a metodologia de pesquisa bibliográfica sobre o tema. A era digital trouxe inúmeras facilidades e oportunidades, mas também novos desafios relacionados à segurança e à cidadania digital. A segurança digital refere-se às medidas para proteger informações e sistemas contra cibercrimes, enquanto a cidadania digital envolve comportamentos éticos no uso de tecnologias. Conclui-se que a promoção dessas práticas requer esforços conjuntos de governos, instituições e indivíduos, com políticas claras, treinamentos regulares e uma cultura de segurança. A adoção de senhas fortes, autenticação de dois fatores e educação contínua são fundamentais. O combate ao cyberbullying, a verificação de informações e a denúncia de abusos são essenciais para um ambiente digital seguro. Este estudo oferece insights e recomendações para criar um ambiente digital mais seguro, ético e

inclusivo para todos.

Palavras-chave: Segurança. Informações. Ético

ABSTRACT

The objective of this study is to analyze the importance of digital security and citizenship, highlighting the main challenges faced and the proposed solutions to overcome them. To achieve these objectives, the bibliographic research methodology on the topic was used. The digital era has brought numerous conveniences and opportunities, but also new challenges related to digital security and citizenship. Digital security refers to measures to protect information and systems against cybercrimes, while digital citizenship involves ethical behaviors in the use of technologies. It is concluded that the promotion of these practices requires joint efforts from governments, institutions, and individuals, with clear policies, regular training, and a culture of security. The adoption of strong passwords, two-factor authentication, and continuous education are fundamental. Combating cyberbullying, verifying information, and reporting abuses are essential for a safe digital environment. This study offers insights and recommendations for creating a safer, more ethical, and inclusive digital environment for all.

Keywords: Security. Information. Ethical.

1 INTRODUÇÃO

A era digital trouxe inúmeras facilidades e oportunidades, transformando a forma como vivemos, trabalhamos e nos comunicamos. No entanto, junto com esses benefícios, surgiram novos desafios, especialmente no que se refere à segurança e à cidadania digital. A segurança digital, que se refere às

medidas e práticas adotadas para proteger informações e sistemas contra acessos não autorizados e cibercrimes, tornou-se um aspecto crítico na sociedade contemporânea. Simultaneamente, a cidadania digital, que envolve o comportamento ético e responsável no uso das tecnologias digitais, é fundamental para garantir que o ambiente online seja seguro e produtivo para todos os usuários.

O objetivo deste estudo é analisar a importância da segurança e da cidadania digital, destacando os principais desafios enfrentados e as soluções propostas para superá-los. Para alcançar esses objetivos, adotamos uma abordagem metodológica fundamentada na pesquisa bibliográfica, revisando artigos, livros e legislações relevantes sobre o tema.

A pesquisa bibliográfica é um método de investigação que envolve a consulta e análise de materiais previamente publicados, como livros, artigos científicos, teses, dissertações, relatórios técnicos e outras obras acadêmicas. Esse tipo de pesquisa tem como objetivo obter um entendimento profundo sobre um tema específico, identificar as principais teorias e conceitos relacionados ao assunto e revisar os avanços e lacunas existentes no conhecimento.

Este trabalho está organizado da seguinte maneira: inicialmente, apresentamos uma visão geral sobre a segurança digital, discutindo os principais princípios e medidas para proteger informações e sistemas. Em seguida, exploramos o conceito de cidadania digital, detalhando os comportamentos éticos e responsáveis que devem ser adotados pelos usuários da internet. Posteriormente, discutimos os desafios e soluções

relacionados à cidadania digital, incluindo o combate ao cyberbullying, a verificação de informações e a denúncia de comportamentos inapropriados. Finalmente, destacamos o papel das instituições educacionais e corporativas, bem como dos indivíduos, na promoção da segurança e cidadania digital, enfatizando a importância de políticas claras, treinamentos regulares e uma cultura de segurança.

2 FUNDAMENTAÇÃO TEÓRICA OU REVISÃO DA LITERATURA

A era digital trouxe inúmeras facilidades e oportunidades, mas também introduziu novos desafios, especialmente no que tange à segurança e à cidadania digital. Segurança digital abrange as medidas e práticas utilizadas para proteger informações e sistemas contra acessos não autorizados e cibercrimes. Cidadania digital envolve o comportamento ético e responsável no uso das tecnologias digitais. A segurança digital é um aspecto crítico na sociedade contemporânea, à medida que a dependência da tecnologia cresce exponencialmente. Segundo Santos, Martins e Tybusch (2017) os crimes cibernéticos e o direito à segurança jurídica são questões emergentes que necessitam de uma análise aprofundada da legislação vigente no cenário brasileiro contemporâneo.

A existência do Direito está associada à jurisdição, e sua função jurisdicional de resolução de conflitos entre pessoas e comunidades no espaço virtual, e de tutela jurisdicional do Poder Público, ou seja, esteja conexa ao Estado. Ao que se trata dos crimes virtuais, são os delitos praticados por meio da Internet que podem ser enquadrados no Código Penal brasileiro, e os infratores estão sujeitos às penas previstas na lei. O Brasil é um país que não

tem uma legislação definida e que abranja, de forma objetiva e geral, os diversos tipos de crimes cibernéticos que ocorrem no dia a dia e que aparecem nos jornais, na televisão, no rádio e nas revistas. Na ausência de uma legislação específica, aquele que praticou algum crime informático deverá ser julgado dentro do próprio Código Penal, mantendo-se as devidas diferenças. Se, por exemplo, um determinado indivíduo danificou ou foi pego em flagrante danificando dados, dados estes que estavam salvos em CDs de sua empresa, o indivíduo deverá responder por ter infringido o artigo 163 do Código Penal, que é ‘destruir, inutilizar ou deteriorar coisa alheia: pena – detenção, de um a seis meses, ou multa’

A legislação brasileira tem evoluído para enfrentar os desafios dos crimes cibernéticos, mas ainda existem lacunas que necessitam de atenção. É essencial que as políticas públicas avancem para cobrir essas brechas, proporcionando um ambiente mais seguro para todos os usuários da internet. Além disso, a cidadania digital é fundamental para garantir que os indivíduos usem a tecnologia de forma ética e responsável. Engloba Inclui a conscientização sobre privacidade, a proteção contra fraudes e a adoção de comportamentos respeitosos e legais no ambiente online. Trentin e Trentin (2012) ressaltam a importância da educação digital, destacando que o desenvolvimento de uma cidadania digital sólida deve ser um esforço coletivo entre governos, instituições educacionais e a sociedade como um todo.

3 METODOLOGIA

A presente pesquisa caracteriza-se como um estudo de natureza bibliográfica, de abordagem qualitativa e de caráter exploratório, tendo como objetivo compreender e analisar a importância da segurança e da cidadania digital no contexto atual da era da informação. A escolha por esse tipo de investigação justifica-se pela necessidade de levantar, sistematizar e refletir criticamente sobre os conhecimentos já produzidos e publicados sobre o tema, a fim de construir uma base teórica sólida que fundamente a discussão proposta.

A coleta de dados foi realizada por meio da seleção e análise de livros, artigos científicos, dissertações, teses, documentos legais e publicações acadêmicas disponíveis em fontes confiáveis, como o Google Acadêmico, Scielo, Portal de Periódicos da CAPES, entre outros repositórios nacionais. A seleção do material seguiu critérios de relevância temática, atualidade — priorizando publicações dos últimos cinco anos — e pertinência ao objeto de estudo, com ênfase em autores brasileiros que abordam as questões da segurança digital, ética nas redes, cidadania digital e os desafios da educação na era da informação.

O procedimento metodológico adotado envolveu uma leitura crítica e interpretativa dos textos selecionados, visando identificar convergências, divergências e lacunas no debate acadêmico sobre o tema. A análise foi feita de forma qualitativa, buscando compreender o conteúdo dos textos e como eles contribuem para o entendimento da construção de uma cultura digital pautada na responsabilidade, respeito, proteção de dados e participação cidadã.

Por se tratar de uma pesquisa exclusivamente bibliográfica, não houve coleta de dados primários, nem aplicação de questionários ou entrevistas com sujeitos. Ainda assim, a sistematização das informações permitiu a construção de uma reflexão aprofundada sobre os principais desafios e possibilidades da cidadania e segurança digital, especialmente no ambiente educacional.

4 RESULTADOS E DISCUSSÕES OU ANÁLISE DOS DADOS

O respeito no mundo digital é tão importante quanto no físico. Tratar os outros com cortesia e consideração, mesmo em desacordos, e evitar comportamentos abusivos como bullying e discurso de ódio são essenciais. A comunicação respeitosa, evitando linguagem ofensiva, e o respeito pela diversidade de opiniões e culturas promovem um ambiente digital harmonioso e inclusivo. A privacidade digital é um direito fundamental. Os usuários devem proteger suas informações pessoais, como senhas e dados financeiros, e respeitar a privacidade alheia, evitando divulgar informações sem consentimento.

Práticas de privacidade incluem o uso de configurações de segurança adequadas e a cautela com solicitações de informações pessoais. A educação digital é crucial para a compreensão das leis, regulamentos e práticas recomendadas no uso da internet. Estar informado sobre direitos autorais, proteção de dados e comportamentos apropriados online é fundamental. Programas de conscientização, workshops e cursos sobre cidadania digital ajudam os usuários a navegar na internet de maneira segura e responsável, mantendo-se atualizados sobre tendências e ameaças cibernéticas.

Conforme Teixeira e Lima (2013, p.15), "a cidadania digital envolve não apenas o uso consciente e responsável das tecnologias, mas também a capacidade de monitorar e contribuir ativamente para a melhoria das cidades e comunidades por meio de dispositivos móveis e outras tecnologias digitais". Os princípios de cidadania digital visam promover um uso consciente, respeitoso e seguro da internet. A responsabilidade, o respeito, a privacidade e a educação são pilares essenciais para garantir que a interação no mundo digital seja positiva e construtiva. Adotar esses princípios contribui para um ambiente online mais seguro, ético e inclusivo para todos.

Os desafios da cidadania digital incluem o combate ao cyberbullying, a proteção contra a disseminação de informações falsas e a garantia de que os direitos dos usuários sejam respeitados. Segundo Trentin e Trentin (2012) a internet possibilitou a publicação de conteúdos ofensivos em redes sociais, resultando em uma necessidade crescente de regulamentações para a proteção contra danos morais. No que tange à responsabilidade do usuário infrator, pode-se observar, diante dos casos apresentados, que este sofrerá a responsabilização pelas informações ilícitas vinculadas no ambiente virtual, e o provedor do site de relacionamento será responsabilizado somente se deixar de excluir ou bloquear as imagens ou informações ofensivas, após transcorrido certo prazo desde a notificação feita pela vítima.

Gagliano e Pamplona Filho (2006, p. 36), caracterizam o dano ou prejuízo como “a lesão a um interesse jurídico tutelado – patrimonial ou não – causado por ação ou omissão do sujeito infrator”.

Facilitar a denúncia de abusos e comportamentos inapropriados online é outra medida importante. Criar mecanismos acessíveis e eficazes para que as pessoas possam reportar esses comportamentos é fundamental para manter um ambiente digital seguro. Plataformas digitais e redes sociais devem proporcionar ferramentas de denúncia claras e facilmente utilizáveis, além de garantir que todas as denúncias sejam tratadas com seriedade e rapidez. A implementação de práticas de segurança e cidadania digital requer um esforço conjunto de governos, instituições e indivíduos. Políticas públicas robustas devem ser estabelecidas para regulamentar o uso da internet e proteger os cidadãos contra ameaças cibernéticas. Programas educacionais que ensinem sobre segurança digital, ética e etiqueta online são essenciais para conscientizar a população. Além disso, a participação ativa de indivíduos, adotando práticas seguras e responsáveis, contribui para a criação de um ambiente digital mais seguro e ético para todos.

Indivíduos também têm responsabilidade na manutenção da segurança digital e prática da cidadania digital. Trentin e Trentin (2012) afirmam que eles devem praticar a autodisciplina, adotando práticas seguras, como a criação de senhas fortes, a atualização regular de softwares e o cuidado ao compartilhar informações pessoais. Educar-se continuamente é outra responsabilidade importante. Manter-se informado sobre as últimas ameaças e boas práticas de segurança permite que os indivíduos estejam preparados para enfrentar novos desafios no ambiente digital. Respeitar os outros é igualmente fundamental. Isso inclui tratar outros usuários com respeito, evitando comportamentos abusivos ou prejudiciais, e denunciando

comportamentos inapropriados quando presenciados. Dessa forma, cada pessoa contribui para um ambiente online mais seguro e ético.

A segurança digital e a cidadania digital são pilares fundamentais para um uso responsável e seguro da internet. Conhecer e aplicar os princípios de segurança digital ajuda a proteger informações e sistemas contra ameaças cibernéticas, enquanto a cidadania digital promove um ambiente online ético e respeitoso. Como destacado por Santos et al. (2017) e Trentin e Trentin (2012) a legislação e as práticas de segurança precisam evoluir continuamente para acompanhar as novas ameaças e desafios do mundo digital. A educação e a conscientização são ferramentas essenciais para garantir que todos os usuários possam navegar na internet de forma segura e responsável.

A importância da segurança digital, nesse sentido, ultrapassa a simples proteção técnica de dados e se consolida como um elemento estruturante da convivência no meio virtual. Conforme Santos, Martins e Tybusch (2017), a compreensão da segurança jurídica no ciberespaço é fundamental para que os usuários tenham confiança nas interações realizadas no ambiente digital, o que impacta diretamente em sua capacidade de exercer a cidadania digital de maneira plena. Sem essa segurança, o ambiente digital torna-se um território propício à violação de direitos, disseminação de conteúdos ilícitos e práticas abusivas, dificultando a construção de uma cultura digital ética e respeitosa.

Ainda segundo os autores, a legislação brasileira, embora tenha avançado em marcos regulatórios como o Marco Civil da Internet (Lei nº

12.965/2014) e a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), enfrenta desafios constantes diante da rapidez com que novas tecnologias surgem e impactam a vida em sociedade. O dinamismo da internet exige que a legislação e as políticas públicas estejam em constante atualização para garantir a proteção dos usuários, especialmente os mais vulneráveis, como crianças, adolescentes e idosos. Trentin e Trentin (2012) destacam que é dever dos usuários conhecer e respeitar essas normas, uma vez que o desconhecimento da legislação não os isenta de responsabilidade por danos causados.

Além disso, como apontam Gagliano e Pamplona Filho (2006), o dano digital não se limita ao aspecto patrimonial, mas abrange também a esfera moral e emocional. Comentários ofensivos, exposição indevida de imagens, perseguições virtuais e falsas acusações podem causar sérios prejuízos à integridade psicológica das vítimas, exigindo uma atuação firme tanto das plataformas digitais quanto dos órgãos públicos. A responsabilização do infrator, portanto, é um passo importante, mas não suficiente: é necessário promover ações preventivas, educativas e estruturais que fortaleçam o senso de responsabilidade e respeito entre os usuários da internet.

Nesse contexto, a educação para a cidadania digital torna-se um caminho imprescindível. Como defendem Teixeira e Lima (2013), educar para a cidadania digital significa formar sujeitos críticos, conscientes de seus direitos e deveres no ambiente virtual, capazes de utilizar as tecnologias de forma ética, responsável e participativa. Isso inclui, por exemplo, desenvolver competências para identificar fake news, praticar o pensamento

crítico diante de conteúdos duvidosos, proteger a própria privacidade e respeitar a privacidade alheia. A escola, nesse processo, tem um papel central, pois é o espaço privilegiado para a formação ética e cidadã.

Trentin e Trentin (2012) reforçam que a responsabilidade dos usuários nas redes sociais deve ser continuamente trabalhada nas instituições educacionais, uma vez que muitos jovens ingressam no universo digital sem preparo adequado, reproduzindo práticas discriminatórias ou abusivas. O uso pedagógico das redes sociais, quando orientado, pode ser uma poderosa ferramenta de aprendizagem e de construção de valores. No entanto, quando utilizado de forma inconsequente, contribui para a normalização de condutas agressivas e para a naturalização de violências simbólicas. Por isso, a mediação ética e pedagógica do uso das tecnologias é fundamental para a promoção de uma cidadania digital efetiva.

A atuação dos gestores educacionais, professores e demais profissionais da educação deve estar voltada à implementação de projetos e ações que integrem a cidadania digital ao currículo escolar, de forma transversal e contextualizada. Programas de formação continuada, como indicam Santos et al. (2017), devem capacitar os educadores para lidar com os desafios contemporâneos do mundo digital, oferecendo subsídios teóricos e práticos para que possam orientar seus alunos sobre questões como segurança online, privacidade, combate ao discurso de ódio e uso ético das mídias. Esses programas, além de ampliar o repertório dos docentes, contribuem para a construção de uma cultura escolar mais segura e acolhedora no ambiente virtual.

Outro ponto relevante é a articulação entre escola, família e comunidade. Gagliano e Pamplona Filho (2006) argumentam que a construção de um ambiente digital seguro e responsável não é uma tarefa exclusiva da escola, mas demanda um esforço coletivo. As famílias precisam estar envolvidas e conscientes de sua função na orientação do uso das tecnologias pelos jovens. É necessário criar canais de comunicação eficazes entre escola e responsáveis, promovendo rodas de conversa, palestras e campanhas de conscientização. O acesso à informação e à formação também deve ser garantido às famílias, de modo a diminuir as desigualdades no uso das tecnologias e promover a inclusão digital com responsabilidade.

Nesse sentido, a inclusão digital precisa vir acompanhada de uma proposta ética e cidadã. Como alertam Teixeira e Lima (2013), não basta garantir o acesso às tecnologias se não forem assegurados também os conhecimentos necessários para que esse uso seja crítico, responsável e transformador. A cidadania digital envolve uma atuação consciente e engajada na esfera pública digital, por meio da participação em debates, do respeito à diversidade e da denúncia de práticas abusivas. Assim, os espaços digitais tornam-se também espaços de exercício democrático, onde os sujeitos podem reivindicar direitos, colaborar com a construção do bem comum e lutar contra as desigualdades.

A proteção dos dados pessoais é outro tema que exige constante atenção. Conforme Santos et al. (2017), com o avanço da tecnologia, os dados dos usuários se tornaram um dos ativos mais valiosos do mundo contemporâneo, sendo frequentemente utilizados por empresas para fins comerciais e por

agentes mal-intencionados para práticas criminosas. O desconhecimento sobre o uso e o destino das informações compartilhadas na internet expõe os usuários a riscos significativos, como fraudes, extorsões e violação de privacidade. Dessa forma, compreender os mecanismos de segurança digital e os direitos assegurados pela LGPD é essencial para a proteção dos usuários e para o fortalecimento da cidadania digital.

Para Trentin e Trentin (2012), a autodisciplina no uso das tecnologias é um elemento-chave na prevenção de incidentes de segurança digital. A criação de senhas seguras, o cuidado com links suspeitos, o uso de antivírus e o controle das permissões de aplicativos são atitudes básicas, mas eficazes, na proteção dos dados pessoais. A prática dessas ações cotidianas deve ser incentivada desde os primeiros contatos com as tecnologias, seja na escola, seja no ambiente familiar. Ao mesmo tempo, a cultura da denúncia precisa ser fortalecida, permitindo que os usuários saibam como reagir diante de conteúdos ofensivos ou de situações de risco.

A construção de uma cultura de segurança e cidadania digital depende da integração entre legislação, educação e conscientização social. Como bem enfatizam Gagliano e Pamplona Filho (2006) e Santos et al. (2017), é necessário que as leis acompanhem a evolução tecnológica, mas também que os indivíduos se tornem protagonistas de sua própria proteção e do cuidado coletivo no ambiente virtual. A cidadania digital, portanto, não se limita ao conhecimento técnico sobre o uso das ferramentas digitais, mas envolve atitudes éticas, respeitosas e comprometidas com o bem-estar comum.

5 CONCLUSÃO

Os objetivos deste estudo foram amplamente atendidos através da análise detalhada da importância da segurança e da cidadania digital, destacando os principais desafios e propondo soluções viáveis para superá-los. Utilizando a metodologia de pesquisa bibliográfica, foi possível identificar as práticas essenciais para proteger informações e sistemas contra cibercrimes e promover comportamentos éticos no uso das tecnologias digitais. Embora a era digital tenha trazido inúmeras facilidades e oportunidades, ela também apresentou desafios significativos que demandam uma abordagem conjunta de governos, instituições e indivíduos.

Conclui-se que a promoção da segurança e da cidadania digital é fundamental para garantir um ambiente online seguro e ético. Implementar medidas como a criação de senhas fortes, o uso de autenticação de dois fatores e a educação contínua é essencial para proteger contra ameaças cibernéticas. Além disso, o combate ao *cyberbullying*, a verificação da veracidade das informações e a facilitação da denúncia de abusos são passos essenciais para criar uma internet mais segura e inclusiva. Este estudo oferece recomendações práticas que podem ser implementadas para alcançar esses objetivos, contribuindo para um uso mais consciente e responsável da tecnologia por todos os usuários.

REFERÊNCIAS BIBLIOGRÁFICAS

GAGLIANO, R.; PAMPLONA FILHO, R. **Direito digital e internet**: proteção e responsabilidade. São Paulo: Atlas, 2006.

SANTOS, M. M.; MARTINS, L. F.; TYBUSCH, A. Crimes cibernéticos e a segurança jurídica. **Revista Brasileira de Direito Digital**, v. 3, n. 2, p. 5–12, 2017.

TEIXEIRA, C. A.; LIMA, J. R. Cidadania digital e inclusão tecnológica. **Revista de Educação e Tecnologia**, v. 9, n. 1, p. 13–20, 2013.

TRENTIN, M.; TRENTIN, P. A responsabilidade dos usuários nas redes sociais. **Revista de Direito Contemporâneo**, v. 5, n. 3, p. 85–94, 2012.

[1] Graduação em Pedagogia pela Universidade do Extremo Sul Catarinense. Graduação em Geografia pela Universidade do Extremo Sul Catarinense. Especialização em Educação Inclusiva pela Universidade de Santa Catarina. Mestrando em Tecnologias Emergentes em Educação pela Must University. E-mail. zulmaguidi@gmail.com