



O PAPEL DA LEGISLAÇÃO BRASILEIRA NA PREVENÇÃO DE INCIDENTES CRIMINAIS EM AMBIENTES ESCOLARES

THE ROLE OF BRAZILIAN LEGISLATION IN PREVENTING CRIMINAL INCIDENTS IN THE SCHOOL ENVIRONMENT

DOI: 10.5281/zenodo.10988842

Laide Daiane Costa Campos¹
Maria Christina Monteiro Vieira²

RESUMO

Este estudo aborda a crescente incidência de práticas criminais em ambientes educacionais, com especial atenção para o uso da deep web como um meio para essas atividades criminosas. O problema de pesquisa se concentra em compreender o impacto dessa realidade virtual na segurança das escolas e identificar medidas eficazes para prevenir e combater esses delitos. O objetivo geral deste estudo é, portanto, investigar o papel da legislação brasileira vigente na prevenção de crimes em ambientes escolares, explorando a influência da deep web. Para alcançar esse objetivo, realizou-se uma revisão bibliográfica, destacando a relevância do estudo, devido à preocupante realidade dos crimes em ambientes educacionais. A deep web emergiu como um espaço propício para a prática desses crimes, fazendo com que se tornasse essencial realizar pesquisas e debates sobre medidas voltadas a reduzir sua ocorrência nas escolas, além de compreender as tendências atuais na utilização dessa plataforma para atividades ilegais. No contexto da legislação vigente, este estudo contribui para a formação de profissionais preparados para lidar com os desafios emergentes da criminalidade na era digital, promovendo ambientes escolares mais seguros.

Palavras-chave: legislação; deep web; segurança escolar; ataques a escolas; prevenção de crimes.

ABSTRACT

- 1 Mestre em Estudos de Linguagem pela Universidade Federal de Mato Grosso (UFMT); graduada em Letras – Língua Portuguesa e Língua Inglesa pela UFMT; especialista em Revisão de Textos pelo Instituto Pedagógico Brasileiro (IPB) e revisora de textos. E-mail: daianecosta10000@gmail.com.
- 2 Especialista em Revisão de Textos; Língua Portuguesa e Literatura Brasileira e Tutoria em Educação à Distância pelo Instituto Pedagógico Brasileiro (IPB); graduada em Letras – Língua Portuguesa e Língua Inglesa pela Universidade Federal de Mato Grosso (UFMT) e revisora de textos. E-mail: mchristinavieira@gmail.com.



This study addresses the growing incidence of criminal practices in educational environments, with particular attention to the use of the Deep Web as a medium for these criminal activities. The research problem focuses on understanding the impact of this virtual reality on school security and identifying effective measures to prevent and combat these crimes. Therefore, the general objective of this study is to investigate the role of the current Brazilian legislation in the prevention of crimes in the school environment, exploring the influence of the Deep Web. To achieve this goal, a literature review was carried out, highlighting the relevance of the study due to the worrying reality of crime in educational environments. The Deep Web has emerged as a favorable space for the practice of these crimes, making it essential to carry out research and debate on measures aimed at reducing their occurrence in schools, as well as to understand current trends in the use of this platform for illegal activities. In the context of current legislation, this study contributes to the training of professionals prepared to deal with the emerging challenges of crime in the digital age, promoting a safer school environment.

Keywords: Legislation; Deep Web; School safety; Attacks on schools; Crime prevention.

Introdução

A crescente utilização da *deep web* como palco para atividades criminosas tem suscitado preocupações significativas, especialmente no contexto dos ambientes educacionais. O uso desse espaço tem impactado profundamente a segurança nas escolas, gerando questionamentos cruciais sobre como enfrentar esse desafio, uma vez que crimes são perpetrados por meio dessa plataforma, que abrangem desde o compartilhamento de conteúdo ilegal até a coordenação de ataques a instituições de ensino, com sérias consequências para os estudantes, professores e demais membros da comunidade escolar.

Nesse contexto complexo, busca-se responder ao seguinte problema de pesquisa: como a utilização da *deep web* afeta a segurança em ambientes educacionais e quais medidas podem ser implementadas para prevenir e combater crimes cometidos por meio dessa plataforma? Compreender o papel da legislação vigente, especialmente no contexto educacional, na prevenção de crimes em ambientes educacionais e o uso da *deep web* para planejar, executar e divulgar esses delitos é o objetivo geral deste estudo, baseando-se em uma visão do estado atual do conhecimento.

Para alcançar esse objetivo, foram estabelecidos objetivos específicos: conhecer os principais tipos de crimes cometidos em ambientes educacionais por meio da *deep web*, descrever as principais consequências desses crimes na segurança dos estudantes, professores



e demais membros da comunidade escolar e discutir sobre as principais medidas de prevenção e combate a crimes nesse ambiente à luz da legislação brasileira vigente.

Assim, a metodologia empregada nesta pesquisa consistiu em realizar uma revisão bibliográfica sobre o papel da legislação existente no Brasil na prevenção de crimes em ambientes educacionais, com um foco específico na utilização da *deep web* como plataforma para planejar, executar e divulgar tais delitos, por meio de buscas sistemáticas em bases de dados relevantes, de publicações ocorridas no período entre 2015 e 2023, incluindo a Scientific Electronic Library Online (SCIELO), o Scholar Google e o catálogo de teses e dissertações da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), utilizando os seguintes descritores: “legislação educacional”, “*deep web*”, “segurança escolar”, “ataques a escolas” e “prevenção de crimes”.

Ratifica-se a relevância do estudo diante do fato de os crimes em ambientes educacionais serem uma realidade preocupante, afetando profundamente a segurança e o bem-estar de todos os envolvidos na comunidade escolar. Questões como bullying, violência física, assédio sexual e outras formas de delinquência têm consequências sérias, exigindo a implementação de ações eficazes de prevenção e combate.

Ademais, no contexto legal, este estudo encontra respaldo, uma vez que por meio do estudo das leis e normas, que regem o comportamento humano em sociedade, bem como do entendimento sobre os meios de aplicação desses dispositivos no combate e na prevenção de crimes, especialmente nos ambientes escolares, possibilita-se que o espaço educacional se torne mais seguro e apto para enfrentar os desafios emergentes na era digital. É crucial que os profissionais da educação estejam preparados para lidar com as novas formas de criminalidade que surgem devido à evolução tecnológica, como os crimes praticados na *deep web*, que impactam o ambiente escolar.

Crimes da *deep web* em ambientes educacionais



A internet é um elemento fundamental no contexto do processo de globalização, que tem provocado transformações nas tradicionais noções de acesso à informação e de ampla liberdade, tais como a expressão, a manifestação e o pensamento, ampliando consideravelmente seus alcances e profundidade.

Vale ressaltar também que, em nosso país, a condução das políticas relacionadas ao funcionamento e ao progresso da internet fica sob a responsabilidade do Comitê Gestor da Internet no Brasil (CGI.br). Esse organismo foi estabelecido pelo Ministério da Ciência e Tecnologia, por meio da Portaria Interministerial n.º 147, de 31/5/1995, cujas disposições foram posteriormente modificadas pelo Decreto Presidencial n.º 4.829, de 3/9/2003 (BRASIL, 1995, 2003).

A principal finalidade do CGI.br é coordenar e consolidar as relações entre o governo e a sociedade, no que se refere aos serviços de internet no território nacional. Além disso, o CGI.br tem como objetivo impulsionar a qualidade técnica, a inovação e a disseminação dos serviços oferecidos.

Em uma análise mais detalhada para o estudo que se apresenta, é relevante compreender a distinção entre a internet e a *World Wide Web*. Embora, muitas vezes, elas sejam utilizadas como sinônimos, a *World Wide Web* (protocolo HTTP) constitui apenas um subconjunto do vasto conteúdo disponível na internet. Outros protocolos da internet incluem o Protocolo de Transferência de Arquivos (FTP³), serviços de e-mail, grupos de notícias, entre outros.

Em meio a esse contexto, emerge a *deep web*, uma parte da internet que não é acessível por meio dos mecanismos de busca convencionais e que requer o uso de ferramentas específicas para ser explorada. Esse segmento da internet é frequentemente associado a atividades criminosas, como venda de drogas, armas, pornografia infantil e outros tipos de crimes, e pode ser definido como:

Páginas de textos, arquivos, muitas vezes de alta qualidade e com autoridade informacional disponíveis na World Wide Web cujos motores de buscas gerais não

3 Do inglês *File Transfer Protocol*.



podem, devido a limitações técnicas, ou não querem, por escolha deliberada, adicionar aos seus índices de páginas Web. Às vezes também é referida como ‘Web Profunda’ ou ‘material escuro’ (MONTEIRO, 2013, p. 24).

Segundo Lash, Horowitz e Richardson (2018), a *deep web* apresenta um ambiente propício para ações ilícitas, pois permite que os criminosos planejem e executem crimes sem deixar rastros, dificultando a atuação das autoridades policiais. Assim, a utilização desse espaço para a prática de crimes tem representado um grande desafio para a segurança em ambientes educacionais, uma vez que estudantes e membros da comunidade escolar podem ser vítimas dessas ações criminosas, tendo em vista que muitos estudantes acessam essa parte da internet sem a orientação adequada e acabam se envolvendo em atividades criminosas sem saber os riscos que correm (TORRES; HADDAD, 2019).

No Brasil, a legislação prevê sanções para crimes cometidos na *deep web*. Segundo o Código Penal brasileiro, a realização de atividades ilícitas na internet, como a divulgação de pornografia infantil e a venda de drogas, é passível de punição (Brasil, 1940). Além disso, o país é signatário de convenções internacionais, como a *Convenção de Budapeste sobre Crime Cibernético*, que prevê a cooperação internacional na investigação e repressão a crimes cometidos na internet (CONSELHO DA EUROPA, 2001).

De acordo com Vignoli e Monteiro (2015), há um consenso na literatura de que se trata de uma parte oculta da internet, caracterizada por um alto nível de criptografia e pela presença de páginas que oferecem produtos e serviços ilícitos. Esse submundo virtual abrange atividades tão perigosas quanto à comercialização de drogas, armas, seres humanos, órgãos e animais raros, além da contratação de assassinos profissionais, das práticas de *snuff*⁴, do recrutamento de terroristas, da exploração de conteúdo pedófilo, dentre outros.

Nesse sentido, é essencial compreender quais são as possibilidades de crimes que podem ser cometidos em ambientes educacionais, por meio da *deep web*, para buscar meios de coibi-los, conforme explicam Torres e Haddad (2019):

4 *Snuff* são filmagens de assassinatos reais, realizadas pelo executor do ato, cuja finalidade é o entretenimento ou a exploração financeira (VIGNOLI; MONTEIRO, 2015).



- Bullying virtual (ou cyberbullying): a *deep web* oferece um ambiente propício para a prática desse crime, diante da possibilidade de acessar fóruns e comunidades que promovem esse tipo de prática e que pode levar a sérios problemas psicológicos e emocionais para as vítimas, minando o bem-estar e a autoestima dos estudantes e comprometendo o ambiente de aprendizado.
- Venda de drogas: o espaço da *deep web* é conhecido por ser um mercado para a venda de drogas, incluindo substâncias ilícitas e medicamentos sem receita médica, que podem chegar às mãos de estudantes e membros da comunidade escolar. O fácil acesso a essas substâncias representa um risco significativo para os estudantes, que podem ser expostos a influências prejudiciais e a consequências devastadoras para sua saúde e bem-estar, além do potencial envolvimento com atividades criminosas.
- Pornografia infantil: a *deep web* é também um dos principais meios de divulgação e distribuição de pornografia infantil porque pode expor crianças e adolescentes a abusos e exploração sexual, contribuindo para traumas psicológicos de longo prazo e destacando a urgência de proteger a segurança das vítimas e combater essas práticas repugnantes.
- Incitação ao ódio: esse espaço pode e tem sido utilizado para propagar mensagens de ódio e violência contra grupos sociais vulneráveis, levando possivelmente a atos de violência e discriminação dentro do espaço escolar, além de criar um ambiente de hostilidade e insegurança nas escolas, prejudicando a harmonia e a inclusão.
- Cyberstalking: é um ambiente em que é possível acessar informações pessoais e privadas de estudantes e membros da comunidade escolar. Isso pode resultar não apenas em perseguição on-line, mas também em outras formas de assédio, comprometendo seriamente a segurança e a privacidade das vítimas, exigindo ações para proteger sua integridade física e emocional.

Merece destaque retomar a acepção do termo bullying, de origem inglesa e sem tradução exata para o português, que é responsável por descrever comportamentos violentos,



geralmente observados no ambiente escolar, mas que podem ocorrer em diversas outras esferas da vida, como na família e no ambiente de trabalho. Nesse sentido, Barbosa (2015) sinaliza que essas ações se caracterizam por serem violentas, intencionais e repetitivas, sem motivação específica ou justificável, tendo como único objetivo o maltrato, a intimidação, a humilhação ou o amedrontamento da vítima.

Com o advento da internet, o conceito de bullying foi ampliado, dando origem ao cyberbullying, uma forma de intimidação que ocorre no ambiente virtual, caracterizado pelo uso da rede mundial de computadores para depreciar, incitar a violência e adulterar fotos e dados pessoais, criando situações de constrangimento psicossocial (GALIA, 2015).

Gália (2015) destaca ainda que essa prática envolve o uso do espaço virtual para intimidar e hostilizar uma pessoa, sendo prevalente em ambientes escolares e em locais de trabalho, onde pode envolver colegas de sala de aula, professores, chefes, subordinados ou, até mesmo, desconhecidos, incluindo, dentre outros, difamação, insultos e ataques covardes.

É importante pontuar que, desde a promulgação da Constituição Federal de 1988 (CF/1988), o Brasil tem buscado estabelecer maior proteção dos direitos fundamentais de seus cidadãos, incluindo os direitos das crianças e dos adolescentes. O Estatuto da Criança e do Adolescente (ECA), promulgado em 1990, é um dos desdobramentos dessa proteção, buscando garantir a segurança e o bem-estar dessa parcela da população contra qualquer forma de negligência, discriminação, exploração, violência, crueldade e opressão.

Embora o ECA não tenha sido especificamente elaborado para lidar com questões relacionadas à segurança escolar, suas disposições abrangentes têm sido invocadas para combater casos de violência física, moral ou psicológica nas instituições de ensino. Já a Lei de Diretrizes e Bases da Educação Nacional (LDB) (Lei n.º 9.394/1996), que estabelece as bases da educação no Brasil, prevê a proteção dos educandos contra qualquer forma de violência física, moral ou psicológica. Essa legislação representa um marco na garantia do direito à educação em um ambiente seguro e propício ao desenvolvimento integral dos estudantes.

Em âmbito internacional, aplicado ao contexto nacional, destaca-se a *Convenção de Budapeste sobre Crime Cibernético*, adotada em 2001 pelo Brasil, que prevê a cooperação



internacional na investigação e na repressão aos crimes cometidos na internet. A convenção estabelece ainda diretrizes para a criminalização de atividades cibernéticas prejudiciais e fornece um quadro para a cooperação entre os Estados signatários no combate ao crime cibernético (CONSELHO DA EUROPA, 2001).

Em 2012, com o advento da Lei de Crimes Cibernéticos (Lei n.º 12.737/2012), também conhecida como Lei Carolina Dieckmann, foi tipificado os crimes cometidos na internet. Com o avanço da tecnologia, surgiram novas formas de delitos, como invasão de dispositivo informático e obtenção não autorizada de dados, exigindo uma legislação específica para enfrentar esses desafios e proteger os cidadãos contra ameaças virtuais (BRASIL, 2012).

Nesse sentido, o Marco Civil da Internet (Lei n.º 12.965/2014) surge em um contexto de crescente utilização da internet e das redes sociais, estabelecendo princípios, garantias, direitos e deveres para os usuários da rede. Essa legislação é fundamental para a proteção dos cidadãos contra abusos on-line, incluindo a responsabilização de provedores de internet e redes sociais por danos decorrentes de conteúdos ilegais gerados por terceiros (BRASIL, 2014).

Outro avanço significativo refere-se à Lei do Bullying Escolar (Lei n.º 13.185/2015), voltada à proteção dos estudantes contra a intimidação sistemática. A referida lei, ao instituir o Programa de Combate à Intimidação Sistemática, mais conhecido como bullying, estabeleceu medidas preventivas e punitivas para combater esse problema que afeta milhares de alunos em todo o país, criando um ambiente mais seguro e saudável nas escolas.

A Lei n.º 13.185/2015 prevê também a capacitação de equipes pedagógicas e docentes, a assistência psicológica, social e jurídica às vítimas e aos agressores e a responsabilização das instituições que não atuarem na conscientização e prevenção do problema. Ela representa um marco legal importante para proteger os estudantes no ambiente educacional digital.

Sobre o Programa de Combate à Intimidação Sistemática, criado em 2015, Freitas (2016) sinaliza que tal programa tem como objetivos a prevenção e o combate ao bullying em todos os espaços reais e virtuais, a capacitação de equipes pedagógicas e docentes, a



assistência psicológica, social e jurídica às vítimas e aos agressores e a responsabilização de instituições que não atuarem na conscientização e na prevenção desse problema.

Outra regulamentação relevante é a Lei Geral de Proteção de Dados (LGPD) (Lei n.º 13.709/2018), que entrou em vigor no Brasil em setembro de 2020. Essa lei estabelece princípios, direitos e deveres para o tratamento de dados pessoais, incluindo aqueles relacionados a estudantes e professores no contexto educacional. Ela exige que as instituições educacionais adotem medidas de segurança adequadas para proteger os dados pessoais de seus membros e estabeleçam políticas claras sobre a coleta e o uso dessas informações. A LGPD também prevê sanções em caso de vazamento de dados pessoais, o que contribui para a segurança digital no ambiente educacional (BRASIL, 2018).

E, mais recentemente, a Lei nº 14.811, de 12 de janeiro de 2024, representa um avanço importante na proteção da criança e do adolescente contra a violência nos estabelecimentos educacionais ou similares. Ao instituir medidas específicas de prevenção e combate à violência, tanto física quanto psicológica, dentro desses ambientes, a lei visa garantir um ambiente seguro e propício ao desenvolvimento educacional e social das crianças e dos adolescentes.

Além disso, a lei prevê a implementação da Política Nacional de Prevenção e Combate ao Abuso e Exploração Sexual da Criança e do Adolescente, reconhecendo a importância de estratégias coordenadas e abrangentes para enfrentar essas formas graves de violência, garantindo o atendimento especializado às vítimas e suas famílias (BRASIL, 2024).

Outro aspecto relevante da Lei nº 14.811/2024 é a sua alteração de dispositivos legais, como o Código Penal (1940) e o ECA (1990), para adequá-los às novas exigências de proteção. A inclusão de dispositivos que aumentam as penalidades para crimes cometidos em instituições de educação básica pública ou privada e a tipificação de condutas como o bullying e o cyberbullying refletem o compromisso do legislativo em adaptar a legislação às novas realidades sociais e tecnológicas, proporcionando uma resposta mais eficaz e abrangente para a proteção das crianças e dos adolescentes no ambiente escolar (BRASIL, 2024).



Diante de todo o exposto, especialmente com a promulgação da Lei nº 14.811/2024, verifica-se um avanço significativo para a garantia da segurança e proteção das crianças e dos adolescentes nos ambientes educacionais. Contudo, é fundamental compreender as consequências e os impactos dessa legislação na segurança escolar. Assim, no próximo tópico, explora-se como essas medidas legais podem influenciar diretamente a prevenção e a resposta a incidentes de violência nas escolas, promovendo um ambiente educacional seguro e acolhedor para todos os estudantes.

Consequências e impactos na segurança escolar

A *deep web* é um segmento da internet que não pode ser indexado por mecanismos de busca convencionais. É um espaço vasto e desconhecido, onde circulam informações e atividades de todos os tipos, incluindo muitas que são ilegais ou nocivas. Para as escolas, esse ambiente representa um risco potencial para a segurança dos alunos, pois, por meio desse espaço, criminosos podem se comunicar e planejar ataques, trocar informações confidenciais ou, até mesmo, vender drogas e armas.

Assim, o acesso desorientado à *deep web* tem provocado efeitos devastadores no ambiente educacional, minando o bem-estar e a qualidade de vida daqueles envolvidos na comunidade escolar e familiar dos estudantes. Dentre os principais riscos da *deep web*, encontram-se os crimes abordados no tópico anterior.

Nesse sentido, o cyberbullying, amplamente disseminado nesse espaço, traz consigo uma série de efeitos nocivos para a segurança dos estudantes. Além de impactar negativamente na autoestima e no bem-estar psicológico das vítimas, o cyberbullying pode comprometer seriamente o ambiente de aprendizado. Os estudantes que sofrem essas agressões virtuais frequentemente experimentam ansiedade, depressão e, em casos extremos, podem ser levados a considerar o suicídio. Esse ambiente hostil também torna mais difícil para os estudantes se concentrarem nos estudos, prejudicando seu desempenho acadêmico.



A venda de drogas e substâncias ilícitas nesse local não indexado é outro crime que apresenta consequências preocupantes para a segurança dos estudantes e os demais membros da comunidade escolar. O fácil acesso a essas substâncias representa um risco significativo para a saúde e o bem-estar dos estudantes.

O uso de drogas ilícitas pode levar a problemas de saúde, dependência, envolvimento em atividades criminosas e, em última instância, ao comprometimento do desenvolvimento educacional e da qualidade de vida. Além disso, a presença dessas substâncias nas escolas cria um ambiente inseguro e pode resultar em conflitos e violência.

No que se refere à disseminação de pornografia infantil na *deep web*, trata-se de outra questão de extrema gravidade que afeta a segurança dos estudantes de maneira profunda. Isso porque a exposição a esse tipo de conteúdo pode causar traumas psicológicos de longo prazo nas vítimas e resultar em uma série de efeitos negativos, como ansiedade, depressão e comportamentos autodestrutivos. Além disso, a exploração sexual de crianças e adolescentes representa uma ameaça real para a segurança física e emocional da comunidade escolar.

A incitação ao ódio dentro desse espaço propaga mensagens de violência e discriminação. Esse ambiente hostil pode levar a atos de violência e conflitos dentro da escola, prejudicando a harmonia e a inclusão. Nesse sentido, merece destaque o caso ocorrido em 13 de março de 2019, na Escola Estadual Raul Brasil, na cidade de Suzano (SP), em que dois alunos, de 17 e 25 anos, armados com revólver, coquetel molotov, arco e flecha e machado, mataram 8 pessoas, deixaram 11 feridas e, em seguida, tiraram suas próprias vidas (TOMAZ; LAVADO; ROHR, 2019).

O resultado das investigações apontou que os assassinos planejaram o crime por mais de um ano e frequentavam fórum na *deep weeb* em busca de conselhos e orientações (Tomaz; Lavado; Rohr, 2019). Diante do fato exposto, é comum nascer um sentimento de insegurança entre os estudantes, que pode resultar em um ambiente de hostilidade e medo, que afeta negativamente a qualidade de vida dos integrantes da comunidade escolar.

O cyberstalking e a violação da privacidade também afetam diretamente a segurança dos estudantes e membros da comunidade escolar. A coleta de informações pessoais e a



perseguição on-line resultam em uma grave violação da privacidade e podem comprometer seriamente a segurança e a paz de espírito das vítimas. O ambiente de hostilidade que essas práticas criam é prejudicial para o bem-estar dos indivíduos e cria um clima de insegurança no ambiente escolar.

Os riscos da *deep web* para a segurança escolar têm o potencial de abalar a confiança dos pais e responsáveis nas instituições de ensino. Compreensivelmente, os pais desempenham um papel crucial na segurança de seus filhos e, quando começam a expressar preocupações com a segurança dos estudantes nas escolas, isso pode levar a várias implicações.

Primeiramente, os pais podem considerar transferir seus filhos para escolas nas quais eles percebam ser mais seguras. Essa decisão pode ser impulsionada por preocupações quanto à exposição de seus filhos a ambientes educacionais nos quais a *deep web* pode representar uma ameaça direta. A perda de estudantes devido a essas preocupações não apenas impacta a receita das escolas, mas também desafia a estabilidade e a qualidade educacional das instituições que enfrentam essa diminuição no número de matrículas.

A segurança dos estudantes sempre foi uma prioridade para as escolas, mas a conscientização sobre os perigos da *deep web* tem intensificado a pressão sobre as instituições para melhorar a segurança. Os pais, agora mais conscientes dessas ameaças, pressionam as escolas para tomarem medidas eficazes a fim de proteger seus filhos. Isso requer um aumento nos recursos alocados à segurança escolar, incluindo tecnologias de segurança cibernética, treinamento para o corpo docente e medidas preventivas para combater ameaças específicas, como o cyberbullying.

Também merece um olhar acurado das escolas a questão de os ataques cibernéticos, o bullying e o assédio levarem a um aumento da violência nas escolas, afetando o clima escolar e a aprendizagem dos alunos. A exposição de estudantes aos perigos desse ambiente pode causar ansiedade, depressão e, em casos extremos, levar ao suicídio.

Quanto ao ambiente de ensino, esse clima hostil pode torná-lo pouco acolhedor e prejudicar o desempenho acadêmico. Além disso, existe a possibilidade de os ataques



cibernéticos resultarem em interrupções no ensino, na perda de dados ou, em situações extremas, em danos físicos às instalações escolares.

Além disso, os impactos dos crimes da *deep web* na segurança escolar podem persistir por muitos anos e afetar a vida adulta dos estudantes. É possível que aqueles que são expostos à violência ou ao assédio na escola passem a enfrentar problemas de saúde mental e de aprendizado em longo prazo. Isso não apenas tem implicações pessoais para esses estudantes, mas também para a sociedade como um todo, uma vez que o impacto negativo em sua educação e bem-estar pode repercutir nas futuras contribuições para a comunidade.

No que diz respeito aos professores, a percepção de que os alunos estão expostos a riscos da *deep web* pode criar um ambiente de trabalho inseguro. Professores que se sentem inseguros em relação à segurança dos estudantes e do ambiente escolar podem ser relutantes em continuar lecionando em escolas onde a segurança é uma preocupação constante.

Assim, resta evidenciado que esse ambiente não indexado representa uma esfera virtual com inúmeras ameaças potenciais para a segurança escolar. Os efeitos prejudiciais da exposição a esses riscos são sentidos não apenas em curto prazo, na forma de impactos psicológicos e sociais imediatos, mas também em longo prazo, à medida que moldam a trajetória de vida dos estudantes e afetam a qualidade geral do ambiente educacional.

Diante desses desafios, é fundamental que escolas e comunidades reconheçam a seriedade dessas questões e se comprometam a adotar estratégias eficazes para garantir um ambiente escolar mais seguro e propício à aprendizagem. Isso inclui a implementação de políticas e regulamentos rígidos para a segurança cibernética, a promoção da conscientização entre estudantes e pais, bem como a oferta de apoio psicológico e social para as vítimas, cuja temática será abordada no próximo tópico.

Medidas de prevenção e combate sob a perspectiva legal

A crescente utilização da *deep web* para atividades criminosas em ambientes educacionais tem gerado uma demanda significativa por medidas de prevenção e combate. Do



ponto de vista da legislação brasileira, várias abordagens podem ser implementadas para enfrentar esse desafio crescente.

Conforme destacado por Campos (2017), uma das estratégias fundamentais para lidar com a ameaça desse espaço nos ambientes educacionais é a promoção de ações educativas, direcionadas aos estudantes e membros da comunidade escolar, sendo ela a mais eficaz para mitigar os riscos associados a esse espaço da internet.

Isso porque, conforme sinalizado por Campos (2017), o entendimento de que a *deep web* pode representar uma ameaça à segurança e ao bem-estar dos envolvidos é o primeiro passo para combater esse problema. Por meio de seminários e palestras conduzidos por especialistas em segurança cibernética, psicólogos e profissionais de Direito, os alunos podem aprender a identificar e a evitar possíveis perigos. Além disso, programas educacionais abrangentes podem ser implementados para introduzir conceitos de segurança digital desde as séries iniciais, capacitando os jovens a navegar na internet de forma segura e consciente.

Também se destaca a necessidade de cooperação entre instituições educacionais e as autoridades policiais como aspecto crucial na prevenção e no combate a crimes na *deep web* (POMPÉO; SEEFELDT, 2013). Nesse sentido, as escolas podem estabelecer parcerias com departamentos de polícia locais e regionais para desenvolver políticas e procedimentos internos que atuem de forma proativa na redução de ameaças.

Essas políticas podem incluir diretrizes para investigar atividades suspeitas relacionadas a esse ambiente não indexado e criar canais de denúncia anônima para que os estudantes e funcionários possam relatar incidentes sem medo de retaliação (CAMPOS, 2017). É essencial que as autoridades policiais estejam atualizadas sobre as tendências do crime nessa plataforma e possam coordenar esforços para combater eficazmente essas ameaças.

Conforme Pompéo e Seefeldt (2013) observaram, a eficácia no crescimento das atividades criminosas transnacionais se deve, em grande parte, à versatilidade e flexibilidade da *deep web*, uma vez que esse ambiente virtual atua como um suporte invisível para as operações criminosas, semelhante a um líquido que se adapta ao ambiente e flui discretamente



por suas margens e infiltrações. Essa ameaça pós-moderna alcança toda a sociedade interconectada, aproveitando-se de uma rede global e silenciosa, em que os envolvidos operam à margem da fiscalização estatal (POMPÉO; SEEFELDT, 2013).

A situação torna-se ainda mais complexa quando vista sob uma perspectiva educacional. A ausência de coordenação e cooperação pode impedir a contenção de crimes que não reconhecem fronteiras, fazendo com que a *deep web* se torne um ambiente fértil e relativamente imune à supervisão estatal, facilitando a disseminação do modus operandi criminoso e a expansão do mercado de crimes nos ambientes educacionais.

Assim, diante da sua capacidade de fornecer um ambiente sigiloso, em que os criminosos podem operar sem serem rastreados, esse ambiente acaba abrigando informações e conteúdos ilícitos, como contrabando, drogas, pedofilia, armas, entre outros, tornando-se um espaço de escolha para aqueles que buscam acessar tais recursos (CAMPOS, 2017).

No trágico caso do massacre na escola em Suzano, de acordo com Tomaz, Lavado e Rohr (2019), suspeita-se que os perpetradores tenham consultado outros criminosos em fóruns da *deep web* dedicados à disseminação de ódio. No entanto, esses crimes representam apenas uma pequena fração do espectro criminal que prospera nesse submundo virtual.

Diante disso, tecnologias e ferramentas específicas podem ser valiosas no esforço de prevenção e combate a crimes nesse ambiente virtual. O'Brien (2018) sugere que softwares de filtragem de conteúdo podem ser usados para bloquear o acesso a sites ilegais na *deep web*, reduzindo a exposição dos estudantes ao conteúdo prejudicial. Além disso, tecnologias de criptografia podem ser empregadas para proteger a privacidade e a segurança dos usuários. O monitoramento de redes também se mostra uma ferramenta importante para identificar e reprimir atividades criminosas desse contexto.

Assim, é relevante destacar que a prevenção e o combate a crimes na *deep web* exigem uma abordagem multidisciplinar. Especialistas em segurança da informação, psicólogos, profissionais do Direito e educadores devem trabalhar juntos para desenvolver estratégias abrangentes. A colaboração entre essas diversas áreas de conhecimento é fundamental para



abordar as complexas questões relacionadas à *deep web* e aos crimes virtuais (O'BRIEN, 2018).

Nesse cenário, o papel da legislação brasileira na implementação e regulamentação dessas medidas é de suma importância para proteger a segurança dos estudantes, professores e membros da comunidade escolar, pois auxilia a garantir o pleno cumprimento dessa responsabilidade. Para tanto, um dos meios vislumbrados é contar com a colaboração de entidades governamentais e não governamentais, incluindo organizações internacionais, ONGs e sociedade civil, todas desempenhando papéis influentes no desmantelamento das engrenagens das práticas criminosas na *deep web*.

Ressalta-se também que a diretriz de prevenção atribuída ao Estado, por meio da CF/1988 e de outras normas vigentes, abrange todos os modos de vulnerabilidade que atingem os estudantes (as vítimas), de forma que o cumprimento de tais preceitos garantidores pelos agentes públicos e escolares deve estar voltado a garantir a esses alunos uma navegação segura pela web.

Ademais, na prevenção voltada às práticas de violência em contextos educacionais, necessário se faz o aperfeiçoamento dos sistemas de coleta de dados e de estatísticas sobre crimes e de instrumentos de monitoramento da efetividade das políticas preventivas adotadas pelos Estados e pelas instituições escolares, tudo visando possibilitar a elaboração e implementação de estratégias válidas de enfrentamento.

Mostra-se essencial compreender ainda que a batalha contra os crimes na *deep web* não é uma responsabilidade exclusiva de nenhuma entidade ou disciplina. É um esforço coletivo, que envolve os educadores, os legisladores, os profissionais da segurança cibernética, os psicólogos, as famílias e, claro, os estudantes.

A conscientização é a chave para preparar as gerações futuras e ajudá-las a navegar por esse ambiente virtual com sabedoria e discernimento. Além disso, é crucial que governos e instituições de ensino promovam um ambiente de aprendizado seguro e responsável, que priorize a segurança dos estudantes em um mundo cada vez mais conectado.



Assim, a abordagem interdisciplinar que envolve educação, segurança, Direito e tecnologia é essencial para enfrentar os desafios que a *deep web* impõe. A colaboração entre essas áreas, juntamente com o apoio de entidades governamentais e não governamentais, é fundamental para construir um ambiente digital mais seguro para as futuras gerações, em que o acesso à informação e à educação coexista com a proteção e a segurança dos estudantes.

Considerações finais

A crescente utilização da *deep web* para atividades criminosas nos ambientes educacionais é uma realidade preocupante, que exige uma abordagem multidisciplinar e cooperativa para prevenção e combate. Este estudo explorou diversas estratégias sob a perspectiva da legislação vigente no país, ressaltando a importância de ações educativas, cooperação entre instituições de ensino e autoridades policiais e o uso de tecnologias para proteger os estudantes contra ameaças nesse ambiente.

A *deep web* é um ambiente virtual complexo, capaz de abrigar uma série de atividades criminosas, desde a disseminação de ódio até a comercialização de produtos ilícitos. Em um mundo cada vez mais conectado, é fundamental que educadores, legisladores, profissionais de segurança cibernética e psicólogos colaborem para criar estratégias abrangentes de prevenção.

A conscientização é a primeira linha de defesa. Educar os estudantes desde tenra idade sobre os riscos da *deep web* é fundamental. Seminários, palestras e programas educacionais podem capacitá-los a navegar de forma segura e consciente, identificando possíveis perigos.

A cooperação entre instituições de ensino e autoridades policiais é outra peça fundamental no quebra-cabeça da prevenção. Políticas internas que investiguem atividades suspeitas relacionadas a esse espaço e canais de denúncia anônima podem reduzir ameaças. As autoridades policiais, por sua vez, devem estar atualizadas sobre as tendências do crime nesse ambiente virtual e coordenar esforços para combater eficazmente essas ameaças.

As tecnologias, como softwares de filtragem de conteúdo e criptografia, desempenham um papel vital na proteção dos estudantes. Elas ajudam a bloquear o acesso a sites ilegais na



deep web e a proteger a privacidade dos usuários. O monitoramento de redes também é uma ferramenta importante para identificar e reprimir atividades criminosas.

Por fim, é importante destacar que a prevenção e o combate a crimes na *deep web* são uma responsabilidade compartilhada. Governos, escolas, profissionais e comunidade devem unir esforços para garantir um ambiente de aprendizado seguro em um mundo digital interconectado. A colaboração entre diversas áreas de conhecimento é essencial para abordar as complexas questões relacionadas à *deep web* e aos crimes virtuais. É uma batalha contínua, que deve ser travada em prol da segurança e do bem-estar dos estudantes e da sociedade como um todo.

Referências

BRASIL. Lei nº 2.848, de 7 de dezembro de 1940. **Código Penal**. Brasília: Senado Federal, 1940.

BRASIL. Lei nº 8.069, de 13 de julho de 1990. **Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências**. Brasília, DF: Presidência da República, Casa Civil, 1990.

BRASIL. Lei nº 9.394, de 20 de dezembro de 1996. **Estabelece as diretrizes e bases da educação nacional (LDB)**. Brasília, DF: Presidência da República, 1996.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências — **Lei de Crimes Cibernéticos**. Brasília, DF: Presidência da República, 2012.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil — **Marco Civil da Internet**. Brasília, DF: Presidência da República, 2014.

BRASIL. Lei nº 13.185, de 6 de novembro de 2015. **Institui o Programa de Combate à Intimidação Sistemática (Bullying)**. Brasília, DF: Presidência da República, 2015.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, DF: Presidência da República, 2018.



BRASIL. **Lei nº 14.811, de 12 de janeiro de 2024.** Institui medidas de proteção à criança e ao adolescente contra a violência nos estabelecimentos educacionais ou similares, prevê a Política Nacional de Prevenção e Combate ao Abuso e Exploração Sexual da Criança e do Adolescente e altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), e as Leis nºs 8.072, de 25 de julho de 1990 (Lei dos Crimes Hediondos), e 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente). Brasília, DF: Presidência da República, 2018.

CAMPOS, P. B. A Deep Web e a segurança nas escolas. **Revista Gestão Educacional**, v. 7, n. 2, p. 143–150, 2017. Disponível em: <https://www.gestaoeducacional.com.br/>. Acesso em: 20 jan. 2024.

CONSELHO DA EUROPA. **Convenção de Budapeste sobre Crime Cibernético.** 2001. Disponível em: <https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168008152c>. Acesso em: 20 jan. 2024.

FREITAS, F. A. C. Comentário sobre a lei “antibullying” Lei n 13.185, de 6 de novembro de 2015 uma tentativa de solução. **Revista Psychiatry on line Brasil**, São Paulo, v. 21, n. 2, 2016. Disponível em: <http://www.polbr.med.br/ano16/pia0216.php>. Acesso em: 10 fev. 2024.

GALIA, R. W. **Cyberbullying:** conceito, caracterização e consequências jurídicas. Disponível em: <http://emporiiododireito.com.br/leitura/cyberbullying-conceito-caracterizacao-e-consequencias-juridicas>. Acesso em: 3 fev. 2024.

LASH, E.; HOROWITZ, J.; RICHARDSON, T. The Dark Side of the Web: An Exploratory Study of the Darknet and its Implications for Policy and Law Enforcement. **Journal of Crime and Justice**, v. 41, n. 4, p. 385–402, 2018.

MONTEIRO, Silvana Drumond. Por uma cartografia conceitual da Web Invisível: a dobra oculta do ciberespaço. **Informação e Sociedade**, João Pessoa, v. 23, n. 3, p. 23-31, set./dez. 2013. Disponível em: <http://www.periodicos.ufpb.br/ojs2/index.php/ies/article/view/16512/10203>. Acesso em: 10 jan. 2024.

O'BRIEN, D. **Staying Safe on the Deep Web.** Security Baron, 2018. Disponível em: <https://securitybaron.com/blog/staying-safe-on-the-deep-web/>. Acesso em: 20 jan. 2024.

POMPÉO, W. A. H.; SEEFELDT, J. P. Nem tudo está no Google: A Deep Web e o perigo da invisibilidade. In: CONGRESSO INTERNACIONAL DE DIREITO E CONTEMPORANEIDADE, 2., 2013, Santa Maria, RS, **Anais [...]**. Santa Maria, RS: UFSM, 2013. p. 436–449. Disponível em: http://coral.ufsm.br/congressodireito/anais/?page_id=82. Acesso em: 22 jan. 2024.



REVISTA OWL (*OWL Journal*)

www.revistaowl.com.br – ISSN: 2965-2634

TOMAZ, K.; LAVADO, T.; ROHR, A. MP de SP apura se organização criminosa na 'deep web' incitou assassinos a cometerem massacre em Suzano. **G1**, São Paulo, 14 mar. 2019. Disponível em: <https://g1.globo.com/sp/sao-paulo/noticia/2019/03/14/mp-de-sp-apura-se-organizacao-criminosa-na-deepweb-incitou-assassinos-a-cometerem-massacre-em-suzano.ghtml>. Acesso em: 23 jan. 2024.

TORRES, R.; HADDAD, E. Deep Web e a segurança digital nas instituições de ensino. **Revista Brasileira de Educação em Segurança Pública**, v. 5, n. 2, p. 117–136, 2019.

VIGNOLI, R. G.; MONTEIRO, S. D. Dark Web e seus não lugares: por um estudo das dobras invisíveis do ciberespaço. The Dark Web and its non-places. **Liinc em Revista**, [s.l.], v. 11, n. 1, p. 140–166, 28 maio 2015. Disponível em: <http://revista.ibict.br/liinc/article/view/3635>. Acesso em: 10 jan. 2024.

Recebido em: 27/02/2024

Aprovado em: 29/03/2024

Publicado em: 14/04/2024