ESTELIONATO VIRTUAL: UM ESTUDO SOBRE A PROTEÇÃO JURÍDICA E DE CONSCIENTIZAÇÃO AOS JOVENS FRENTE AOS CRIMES CIBERNÉTICOS

VIRTUAL FRAUD: A STUDY ON LEGAL PROTECTION AND AWARENESS OF YOUNG PEOPLE AGAINST CYBERCRIMES

Claudia Gonçalves Cassimiro[1]
Emerson Barcelos dos Reis[2]
Gabriel dos Santos Coelho[3]
Gabriela Oliveira Costa Dias[4]
Helen Maria Ferreira Matos[5]
Heitor Araújo Neves[6]
Maria Eduarda Alves Pereira[7]
Maria Rita de Almeida Cecilio[8]
Micaelly Ágatha da Silva Ribeiro[9]
Nayara Aparecida Correia da Silva[10]
Malaquias Felipe Moura Silva[11]

RESUMO

O presente trabalho tem como foco a conscientização dos jovens frente aos crimes virtuais, com ênfase no crime de estelionato. A escolha do tema se justifica pela crescente incidência de fraudes digitais e pela vulnerabilidade dos jovens, que por estarem constantemente conectados à internet e redes sociais, tornam-se alvos fáceis para golpistas. Muitos ainda não possuem o discernimento necessário para identificar situações suspeitas, o que reforça a necessidade de ações educativas preventivas. A relevância social do trabalho está na promoção da informação como ferramenta de proteção, contribuindo para a formação de cidadãos mais críticos e conscientes no uso das tecnologias. A prevenção ao estelionato virtual vai além da segurança individual, pois reduz os impactos coletivos desses crimes, como prejuízos financeiros e danos psicológicos. O projeto foi aplicado na Escola Estadual Ângela Maria, com alunos do ensino médio, por meio de uma palestra educativa que abordou de forma clara e acessível os principais tipos de golpes virtuais, suas consequências e formas de prevenção. A metodologia escolhida permitiu a interação dos alunos, que compartilharam dúvidas e experiências, enriquecendo o debate. O impacto foi significativo, visto que os estudantes demonstraram maior entendimento sobre o tema e relataram mudanças em seus comportamentos digitais. Muitos afirmaram que repassariam o conhecimento adquirido a familiares e amigos, ampliando o alcance da conscientização. Dessa forma, o trabalho cumpriu seu objetivo de educar e prevenir, contribuindo para uma sociedade mais segura e informada.

PALAVRAS-CHAVE: Jovens, estelionato virtual, conscientização, vulnerabilidade, segurança.

[1]Graduando no curso de Direito pela Faculdade Católica de Pará de Minas (FAPAM).
[2]Graduando no curso de Direito pela Faculdade Católica de Pará de Minas (FAPAM).
[3]Graduando no curso de Direito pela Faculdade Católica de Pará de Minas (FAPAM).
[4]Graduando no curso de Direito pela Faculdade Católica de Pará de Minas (FAPAM).
[5]Graduando no curso de Direito pela Faculdade Católica de Pará de Minas (FAPAM).
[6]Graduando no curso de Direito pela Faculdade Católica de Pará de Minas (FAPAM).
[7]Graduando no curso de Direito pela Faculdade Católica de Pará de Minas (FAPAM).
[8]Graduando no curso de Direito pela Faculdade Católica de Pará de Minas (FAPAM).
[9]Graduando no curso de Direito pela Faculdade Católica de Pará de Minas (FAPAM).
[10]Graduando no curso de Direito pela Faculdade Católica de Pará de Minas (FAPAM).
[11]Graduando no curso de Direito pela Faculdade Católica de Pará de Minas (FAPAM).

ABSTRACT

This work focuses on raising awareness among young people about cybercrimes, with an emphasis on fraud. The choice of the topic is justified by the growing incidence of digital fraud and the vulnerability of young people, who, because they are constantly connected to the internet and social networks, become easy targets for scammers. Many still do not have the necessary discernment to identify suspicious situations, which reinforces the need for preventive educational actions. The social relevance of the work lies in the promotion of information as a protection tool, contributing to the formation of citizens who are more critical and aware in the use of technologies. Preventing cyberfraud goes beyond individual security, as it reduces the collective impacts of these crimes, such as financial losses and psychological damage. The project was implemented at the Ângela Maria State School, with high school students, through an educational lecture that addressed in a clear and accessible way the main types of cyber scams, their consequences and ways of preventing them. The chosen methodology allowed interaction between students, who shared questions and experiences, enriching the debate. The impact was significant, as students demonstrated greater understanding of the topic and reported changes in their digital behaviors. Many said they would pass on the knowledge they had acquired to family and friends, thus increasing awareness. In this way, the work fulfilled its objective of educating and preventing, contributing to a safer and more informed society.

KEYWORDS: young people, cyber fraud, awareness, vulnerability, security

1 INTRODUÇÃO

Com o avanço acelerado das tecnologias digitais, a internet tornou-se um ambiente central para a realização de atividades cotidianas, desde transações bancárias até relações sociais e profissionais. No entanto, essa digitalização em massa também trouxe consigo uma série de consequências negativas, entre as quais se destaca o crescimento expressivo do estelionato virtual. Golpes aplicados por meios eletrônicos, como fraudes bancárias, falsas promessas de vendas e sequestro de dados, têm afetado milhares de brasileiros diariamente, tornando evidente a urgência de tratar o tema com seriedade.

A legislação brasileira, infelizmente, não tem acompanhado na mesma velocidade essa transformação digital. O Direito, por sua natureza mais conservadora e reativa, enfrenta dificuldades para criar e atualizar normas capazes de lidar com os desafios específicos do ambiente virtual. A defasagem entre o desenvolvimento tecnológico e a resposta legislativa acaba por criar brechas legais que facilitam a ação de criminosos e dificultam a responsabilização efetiva dos autores desses delitos.

Além disso, a ausência de políticas públicas amplas de prevenção torna ainda mais grave a situação de grupos vulneráveis, como idosos, os menores, pessoas com baixa escolaridade ou com pouco domínio tecnológico, que frequentemente se tornam alvos preferenciais desses golpes. Nesse contexto, torna-se essencial a implementação de medidas educativas, campanhas de conscientização e o fortalecimento da segurança no ambiente virtual como forma de mitigar os riscos e proteger a população, principal-mente os mais jovens que estão em constante contato com o meio virtual.

2 OBJETIVO

A finalidade central é realizar uma análise sucinta das práticas mais recorrentes de estelionato virtual, com ênfase nas estratégias adotadas pelos criminosos cibernéticos, conhecidos como “catfishers” ou golpistas virtuais. A pesquisa busca compreender as principais formas de estelionato virtual e os mecanismos utilizados por esses indivíduos para enganar e obter vantagens indevidas de suas vítimas que na maioria das vezes são adolescentes e crianças.

Adicionalmente, este trabalho visa a promoção de estratégias preventivas, com ênfase na educação digital, para a conscientização de grupos vulneráveis, como idosos, jovens e pessoas com baixo nível de escolaridade digital, capacitando-os a identificar fraudes e adotar práticas seguras, reduzindo os riscos de estelionato virtual e promovendo uma navegação mais segura.

O avanço da tecnologia e a crescente utilização da internet para atividades cotidianas, como compras, serviços bancários e interações sociais, trouxeram benefícios, mas também ampliaram as oportunidades para a prática de crimes cibernéticos, especialmente o estelionato virtual.

Esse tipo de crime, caracterizado pela fraude por meios eletrônicos, tem se tornado cada vez mais frequente e prejudicial, afetando principalmente aqueles sem conhecimento suficiente para identificarem riscos e se protegerem adequadamente.

Este estudo visa investigar os problemas decorrentes do estelionato virtual, analisando suas formas e os mecanismos subjacentes à fraude digital. Além disso, o projeto busca conscientizar o público sobre os perigos desse crime e apresentar estratégias eficazes de prevenção.

A pesquisa será focada em identificar as principais vulnerabilidades que tornam as pessoas suscetíveis a golpes e nas melhores práticas para se protegerem online. Por meio de palestras educativas, o grupo pretende divulgar o conhecimento sobre os riscos do estelionato virtual, especialmente entre os grupos mais vulneráveis, como idosos e jovens.

Para alcançar uma educação virtual como objetivo central, é pertinente considerar o público alvo mais vulnerável aos meios fraudulentos. Nesse contexto, a disseminação do conhecimento pode ser realizada por meio de publicações, cartilhas informativas e palestras, com o objetivo de apresentar de forma clara e acessível as estratégias de prevenção, os cuidados necessários durante a navegação na internet e as formas de identificar tentativas de fraude.

3 JUSTIFICATIVA

A pesquisa proposta investiga e analisa estratégias para combater o estelionato virtual direcionado ao público mais vulnerável, especialmente os jovens, que apresentam maior interconexão com os meios digitais e maior acessibilidade às tecnologias.

O estudo examina casos em que os jovens se configuram como vítimas potenciais, devido à familiaridade crescente com as novas tecnologias digitais. Além disso, a pesquisa avalia as políticas públicas, legislações e artigos científicos recentes, com foco no marco temporal dos últimos cinco anos, no que tange à proteção dos jovens contra esse tipo de crime e à eficácia das medidas de conscientização.

A pesquisa apresenta uma problemática de investigar e analisar estratégias para combater o estelionato virtual direcionado ao público mais vulnerável, especialmente os jovens, que apresentam maior interconexão com os meios digitais e maior acessibilidade às tecnologias. O estudo examina casos em que os jovens se configuram como vítimas potenciais, devido à familiaridade crescente com as novas tecnologias digitais.

Pois, a crescente digitalização das atividades cotidianas tem proporcionado benefícios, mas também trouxe desafios, especialmente no que diz respeito à segurança online. O estelionato virtual, um crime eletrônico, emergiu como uma das principais ameaças, afetando milhões de pessoas.

Esse crime abrange diversas fraudes, em plataformas digitais, e tem se tornado mais difícil de ser combatido devido à sofisticação dos criminosos e à falta de conhecimento técnico da maioria dos internautas.

O estudo visa identificar as formas mais comuns de estelionato virtual e propor soluções práticas para prevenir tais crimes. A conscientização sobre segurança digital é essencial para reduzir a vitimização, especialmente entre grupos vulneráveis. Além disso, o estudo enfatiza a importância de campanhas educativas para promover atitudes mais seguras na navegação online.

A fundamentação teórica inclui estudos sobre criminologia cibernética e os impactos psicológicos do estelionato virtual, destacando a necessidade de adotar estratégias tecnológicas e educativas para combater o crime e proteger os cidadãos no ambiente digital.

4 METODOLOGIA

Em consideração a seguinte problemática do estelionato virtual, investigando e analisando estratégias para combater esse crime, especialmente em relação ao público mais vulnerável, com ênfase nos jovens, que possuem maior conexão com os meios digitais e maior acessibilidade às tecnologias. O estudo examina casos em que os jovens se configuram como vítimas potenciais, em razão da crescente familiaridade com as novas tecnologias digitais.

A metodologia de pesquisa adotada consiste em uma revisão integrativa da literatura, baseada em artigos científicos, livros, legislações federais e fontes disponíveis em bases de dados acadêmicas, como CAPES, SciELO, entre outras fontes virtuais. Essa abordagem permitirá a análise crítica e a síntese de informações relevantes sobre o tema, contribuindo para a compreensão aprofundada da problemática em questão.

No que tange às fontes e à metodologia aplicada, a pesquisa terá como ênfase um marco temporal de cinco anos, priorizando artigos e outros conteúdos recentes. Esse recorte temporal visa garantir a atualidade e relevância das informações, permitindo uma análise aprofundada das questões contemporâneas relacionadas ao tema em estudo.

Ademais, o Projeto Integrador da Faculdade de Pará de Minas (FAPAM) focará na aplicabilidade social do tema, utilizando publicações virtuais e palestras de conscientização voltadas a jovens vulneráveis. As atividades serão, preferencialmente, realizadas na Escola Estadual Nossa Senhora Auxiliadora, com o objetivo de promover a educação digital e prevenir os riscos do estelionato virtual e adotar práticas seguras no ambiente digital, com a finalidade de reduzir os riscos associados aos meios fraudulentos virtual e promover uma navegação mais segura e informada.

Objetivo Geral:

O avanço tecnológico e a crescente utilização da internet para atividades cotidianas, como compras, serviços bancários e interações sociais, têm proporcionado inúmeros benefícios, mas também gerado novas oportunidades para a prática de crimes cibernéticos, especialmente o estelionato virtual.

Esse tipo de crime, caracterizado por fraudes realizadas por meio de meios eletrônicos, tem se tornado cada vez mais frequente e prejudicial, afetando principalmente indivíduos que carecem de conhecimentos adequados para identificar os riscos e se proteger de maneira eficaz.

O objetivo central deste trabalho é investigar os problemas decorrentes do estelionato virtual, analisando as diversas formas que esse crime pode assumir e os mecanismos que sustentam as fraudes no ambiente digital. Além disso, a pesquisa visa conscientizar o público sobre os perigos associados a esse tipo de crime, propondo estratégias eficazes de prevenção.

O estudo se concentrará na identificação das principais vulnerabilidades que tornam as pessoas suscetíveis a golpes, além de apresentar as melhores práticas para a proteção online.

Objetivos Específicos:

- Conscientização e Prevenção: A principal estratégia a ser promovida por meio deste trabalho é a conscientização dos jovens acerca dos riscos das fraudes online. A realização de palestras sobre segurança digital tem o potencial de disseminar informações essenciais sobre como identificar e evitar golpes, além de orientar o público sobre práticas de proteção de dados pessoais e informações sensíveis.

- Uso de Ferramentas de Segurança: É crucial alertar sobre o público-alvo mais vulnerável ao estelionato virtual, especialmente aqueles envolvidos na compra e venda de produtos online, que frequentemente são atraídos por ofertas tentadoras, mas fraudulentas. A utilização de

ferramentas de segurança digital, como antivírus e sistemas de autenticação, pode reduzir a exposição aos riscos desses golpes.

- Denúncia de Crimes: Orientar a população sobre os canais adequados para denunciar crimes cibernéticos é fundamental. A divulgação de informações sobre como registrar uma denúncia na polícia, em delegacias locais e em órgãos de defesa do consumidor, é essencial para garantir que os crimes sejam investigados e que os criminosos sejam devidamente responsabilizados.

5 DESENVOLVIMENTO

A INTERNET: DA REVOLUÇAÕ DIGITAL À ASCENSÃODO ESTELIONATO VIRTUAL

A internet surgiu como uma ferramenta revolucionária de comunicação e acesso à informação, transformando radicalmente as relações sociais, econômicas e culturais. Desde sua origem militar e acadêmica até sua popularização global, a rede mundial de computadores proporcionou avanços significativos. No entanto, com o crescimento exponencial do ambiente digital, também emergiram novos desafios e riscos, entre eles o aumento dos crimes cibernéticos, com destaque para o estelionato virtual, uma das fraudes mais recorrentes na atualidade.

A internet nasceu na década de 1960, como ARPANET, projeto do Departamento de Defesa dos EUA voltado à comunicação segura entre centros de pesquisa. Com o passar dos anos, evoluiu para uma rede global aberta, ganhando força nos anos 1990 com a criação da World Wide Web e o avanço das tecnologias de conexão. Hoje, a internet é parte integrante do cotidiano, conectando bilhões de pessoas.

Apesar dos inúmeros benefícios, a internet também se tornou um campo fértil para atividades ilícitas. A anonimidade, a dificuldade de rastreamento e a falta de legislação uniforme entre países criaram um ambiente propício para crimes cibernéticos. Entre os mais frequentes estão o roubo de dados, invasões de sistemas, fraudes financeiras e o estelionato virtual que consiste no objeto de pesquisa deste trabalho.

O ESTELIONATO VIRTUAL

O Estelionato virtual consiste em enganar alguém para obter vantagem ilícita, geralmente financeira, por meio de meios digitais. Práticas como phishing, golpes via redes sociais, falsas lojas virtuais e fraudes com boletos bancários têm vitimado milhares de pessoas. O crescimento desse tipo de crime reflete tanto o avanço tecnológico quanto a falta de educação digital e mecanismos eficazes de fiscalização.

Ele se baseia na manipulação da confiança da vítima para aplicar golpes pela internet, seja por e-mail, redes sociais, aplicativos de mensagens, sites falsos ou outras plataformas online e com o crescimento da digitalização e o aumento da presença das pessoas no ambiente virtual, o estelionato digital tem se tornado cada vez mais frequente e sofisticado. Golpistas utilizam diversas técnicas para enganar as vítimas, explorando desde a curiosidade até a fragilidade emocional ou financeira.

O desenvolvimento da internet é uma das maiores conquistas da era moderna, mas também trouxe consigo complexos desafios, especialmente no campo da segurança digital. O estelionato virtual é um exemplo claro de como a tecnologia, se mal utilizada, pode causar danos profundos a indivíduos e à sociedade. Para enfrentar essa realidade, é fundamental investir em educação digital, atualização constante da legislação e ferramentas de proteção cibernética. Somente com uma abordagem integrada será possível reduzir os impactos negativos da era digital

PRINCIPAIS TIPOS DE ESTELIONATO VIRTUAL

1. Phishing

   Consiste em mensagens fraudulentas (por e-mail, SMS ou WhatsApp) que se passam por empresas ou instituições confiáveis para roubar dados pessoais, como senhas, números de cartão de crédito e informações bancárias.

2. Falsas Lojas Virtuais

   Criminosos criam sites com aparência profissional, ofertando produtos com preços atrativos. Após o pagamento, o produto nunca é entregue, e o site costuma sair do ar pouco tempo depois.

3. Golpes em Redes Sociais

   Envolve perfis falsos ou contas invadidas que pedem dinheiro emprestado, vendem produtos inexistentes ou oferecem falsas oportunidades de investimento.

4. Clonagem de WhatsApp

   Os golpistas se passam pela vítima e pedem dinheiro a contatos próximos. A clonagem pode ocorrer após obterem um código de verificação que a vítima fornece sem perceber que está sendo enganada.

5. Boletos Falsos

   São enviados boletos com dados adulterados para desviar o valor do pagamento para contas de criminosos. Isso pode ocorrer por e-mail ou até em sites falsos de empresas reais.

COMO SE PREVINIR DO ESTELIONATO VIRTUAL

- Desconfie de ofertas boas demais para ser verdade: preços muito baixos, promessas de lucro rápido e facilidades incomuns devem levantar suspeitas.
- Não clique em links suspeitos: verifique sempre o remetente e a URL dos sites antes de inserir dados pessoais.
- Use autenticação em dois fatores: essa camada extra de segurança dificulta o acesso de criminosos às suas contas, mesmo que obtenham sua senha.
- Verifique a autenticidade de sites e contatos: prefira acessar sites digitando o endereço diretamente no navegador e confirme dados bancários antes de fazer transferências.
- Atualize seus dispositivos e programas: manter o sistema operacional, antivírus e aplicativos atualizados reduz as vulnerabilidades.
- Eduque-se e eduque os outros: muitos golpes se baseiam em engenharia social, então o conhecimento é uma das maiores defesas.

A lei dos crimes cibernéticos (lei nº 12.737/2012) – O caso Carolina Dieckman

A Lei nº 12.737, sancionada em 30 de novembro de 2012, é um marco na legislação brasileira que trata dos crimes cibernéticos. Conhecida popularmente como a “Lei Carolina Dieckmann”, a norma foi criada em resposta ao aumento de delitos cometidos no ambiente virtual, visando proteger os usuários da internet contra ações nocivas e garantir a integridade de dados pessoais. O nome da lei se deve ao famoso caso da atriz Carolina Dieckmann, que em 2012 teve fotos íntimas vazadas na internet, o que chamou a atenção da sociedade e gerou um clamor por medidas mais eficazes de proteção à privacidade.

A lei tipifica diversos crimes relacionados à invasão de dispositivos eletrônicos, à violação de dados e à disseminação de conteúdo não autorizados. Um dos pontos centrais da legislação é o artigo 154-A, que estabelece a penalidade para quem invadir um dispositivo informático alheio, seja com a intenção de obter, adulterar ou destruir dados. As penas podem variar de três meses a um ano de detenção, além de multa, dependendo da gravidade do ato. Este dispositivo legal surgiu como uma resposta direta a casos como o de Carolina Dieckmann, que evidencia as vulnerabilidades enfrentadas por indivíduos em um mundo cada vez mais digital (Costa, 2020).

O caso de Carolina Dieckmann destacou a necessidade de um marco legal que protegesse não apenas as figuras públicas, mas todos os cidadãos de ações criminosas que possam ocorrer na internet. A repercussão do episódio mobilizou a opinião pública e evidenciou a fragilidade das legislações

existentes em relação à proteção da privacidade e à segurança de dados pessoais. Conforme relata Ribeiro (2019), o episódio não apenas expôs a atriz a constrangimentos, mas também gerou uma reflexão profunda sobre os limites da privacidade na era digital e a responsabilidade dos provedores de serviços online.

A promulgação da Lei nº 12.737/2012 foi um passo importante, mas a implementação e a efetividade das punições ainda são questões que desafiam as autoridades. Apesar de a lei prever penalidades, a dificuldade de investigação e a identificação dos autores de crimes cibernéticos muitas vezes limitam a aplicação das sanções. Além disso, a evolução constante da tecnologia traz novos desafios que exigem uma atualização contínua da legislação. Segundo Almeida (2021), a luta contra os crimes cibernéticos é um processo dinâmico, e é fundamental que as leis acompanhem o avanço tecnológico para garantir a proteção dos cidadãos.

Além da lei, o caso Carolina Dieckmann também trouxe à tona a importância da educação digital e da conscientização sobre os riscos envolvidos na utilização da internet. A prevenção, por meio da informação e do conhecimento, é uma ferramenta essencial para que os usuários estejam mais preparados para evitar situações de vulnerabilidade. De acordo com Souza (2022), iniciativas de conscientização são cruciais para formar cidadãos mais críticos e atentos aos seus direitos e deveres no ambiente digital.

Em conclusão, a Lei nº 12.737/2012 representa um avanço significativo na proteção dos direitos dos cidadãos no espaço virtual, especialmente em um contexto onde crimes cibernéticos se tornaram uma preocupação crescente. O caso de Carolina Dieckmann catalisou a discussão sobre a necessidade de legislação específica e a importância da proteção da privacidade. No entanto, é necessário que a lei seja efetivamente aplicada e que haja um esforço contínuo para educar a população sobre os riscos da internet e a importância de proteger seus dados pessoais.

O Marco Civil da Internet (lei nº 12.965/2014) e a proteção de dados dos usuários

Em 2014, foi sancionada a Lei nº 12.965, também conhecida como a Lei do Marco Civil da Internet, que trouxe princípios, direitos, garantias e deveres dos usuários da internet. O crime de estelionato tipificado no artigo 171 do Código Penal brasileiro, obter para si ou para outra vantagem ilícita mediante ardil, artificio, meio fraudulento em prejuízo de outrem. A principal característica do estelionato é manter a vítima em erro e deixá-la no prejuízo. No que tange o estelionato virtual, a única diferença havida entre o estelionato virtual e o real, é o modus operandi, pois o virtual necessita do uso de um equipamento de informática. Para este não há qualquer tipificação no ordenamento jurídico, a qual não pode haver qualquer condenação. Maia (2017, p. 76), afirma que o Marco Civil se assenta em três pilares: “a garantia da neutralidade da rede; proteção à privacidade do usuário da Internet; e a garantia da liberdade de expressão”.

O Marco Civil da Internet, estabelecido pela Lei nº 12.965/2014, representa um avanço significativo na regulamentação do uso da internet no Brasil. Essa legislação foi criada com o intuito de garantir os direitos dos usuários na rede, promovendo a liberdade de expressão, a privacidade, e a proteção de dados pessoais. A lei surgiu em um contexto em que a expansão da internet e a crescente digitalização das relações sociais e comerciais levantaram preocupações sobre a segurança e a privacidade dos dados dos usuários (Mendes, 2020).

Um dos principais objetivos do Marco Civil da Internet é assegurar a proteção da privacidade e dos dados pessoais dos internautas. De acordo com o artigo 7º, a lei estabelece que é assegurado ao usuário o direito à proteção de seus dados pessoais, sendo obrigatória a obtenção de consentimento para a coleta, uso e tratamento dessas informações. Essa abordagem reforça a ideia de que os dados dos usuários são uma extensão de sua identidade e, portanto, devem ser tratados com respeito e cuidado. Segundo Silva (2021), essa proteção é crucial em um cenário onde dados pessoais são frequentemente utilizados para fins comerciais sem o consentimento adequado dos titulares.

Além disso, a lei também define a responsabilidade dos provedores de serviço em relação à segurança dos dados que armazenam. O artigo 14 estabelece que esses provedores são responsáveis por danos causados por conteúdo gerado por terceiros, salvo se comprovada a ausência de culpa. Essa disposição busca garantir que os provedores adotem medidas eficazes de segurança e que os usuários sejam informados sobre as políticas de privacidade e de proteção de dados aplicáveis a suas informações pessoais (Costa, 2022).

O Marco Civil da Internet também criou um ambiente propício para a discussão e a formulação de políticas públicas relacionadas à proteção de dados. A Lei Geral de Proteção de Dados (LGPD), que entrou em vigor em 2020, é um desdobramento do Marco Civil, complementando as disposições sobre a proteção de dados pessoais. A LGPD estabelece princípios e diretrizes mais abrangentes, garantindo um maior controle dos usuários sobre suas informações e impondo obrigações rigorosas às empresas que lidam com dados pessoais. A relação entre o Marco Civil e a LGPD reforça a necessidade de um marco regulatório robusto e coeso para a proteção da privacidade e dos dados na era digital (Almeida, 2021).

A efetividade do Marco Civil da Internet na proteção de dados dos usuários também depende da conscientização e da educação digital. Muitos usuários ainda não estão plenamente cientes de seus direitos ou das implicações do compartilhamento de seus dados pessoais na internet. Portanto, campanhas de conscientização são fundamentais para empoderar os cidadãos e permitir que façam escolhas informadas sobre a privacidade e a segurança de suas informações. Como observado por Oliveira (2022), a educação digital deve ser parte integrante da discussão sobre proteção de dados, capacitando os usuários a compreenderem melhor os riscos envolvidos na navegação online.

Em síntese, o Marco Civil da Internet (Lei nº 12.965/2014) representa um marco significativo na

proteção dos direitos dos usuários na internet, com ênfase na proteção de dados pessoais e na privacidade. A inter-relação com a LGPD e a necessidade de conscientização digital reforçam a importância de uma abordagem integrada para garantir a segurança e a privacidade dos internautas. Embora a legislação tenha avançado, a implementação efetiva das normas e a educação dos usuários são essenciais para assegurar que os direitos digitais sejam respeitados e protegidos.

A NECESSIDADE DA EDUCACAÇÃO DIGITAL COMO FORMA DE PREVENÇÃO AO ESTELIONATO VIRTAL

Nos dias de hoje, com o avanço acelerado da tecnologia e o uso constante da internet em praticamente todos os aspectos da vida, é impossível ignorar os riscos que surgem junto com esses benefícios. Um dos problemas mais recorrentes atualmente é o estelionato virtual – os famosos golpes aplicados pela internet. Infelizmente, muitas pessoas ainda caem nessas armadilhas por falta de conhecimento, o que evidencia a importância urgente da educação digital.

A educação digital não se resume apenas a aprender a mexer em um computador ou celular. Ela envolve saber como navegar com segurança, reconhecer ameaças, proteger informações pessoais e entender os limites e responsabilidades no ambiente virtual. É nesse ponto que a prevenção começa: quanto mais informada a pessoa estiver, menor a chance de ser enganada.

Golpes como phishing, clonagem de WhatsApp, falsas promoções, links maliciosos e sites falsos se aproveitam justamente da falta de atenção ou da ingenuidade das vítimas. Muitas vezes, essas vítimas são idosos, jovens, ou até mesmo adultos com pouca familiaridade com o mundo digital. Por isso, investir em programas de conscientização, palestras, campanhas educativas e até mesmo conteúdos acessíveis nas redes sociais é essencial.

Além disso, a educação digital deve começar desde cedo, nas escolas, e ser reforçada nas empresas e comunidades. É preciso criar uma cultura de segurança digital, onde as pessoas sintam confiança em usar a internet, mas também saibam que é preciso cuidado. Do mesmo jeito que aprendemos a nos proteger nas ruas, também temos que aprender a nos proteger online.

Em resumo, a educação digital é uma das armas mais eficazes contra o estelionato virtual. Quando o conhecimento chega antes do golpe, ele tem muito menos chance de dar certo. E cabe a todos nós – educadores, profissionais de tecnologia, instituições públicas e privadas – promover esse conhecimento e fazer com que a internet seja um espaço mais seguro para todos.

6 APLICAÇÃO

No dia 06 de junho de 2025, das 21h às 22h, foi realizado um projeto de extensão universitária com a aplicação de uma palestra educativa ministrada pelos alunos do 6º período do curso de Direito da

FAPAM. A ação teve como objetivo principal orientar e conscientizar a comunidade escolar sobre os cuidados e formas de prevenção contra crimes de estelionato virtual, uma prática criminosa cada vez mais presente no cotidiano digital.

A atividade aconteceu em uma escola local, onde fomos recebidos calorosamente pela vice-diretora Aline Batista, que demonstrou grande interesse pela temática e apoio à proposta educativa. Durante a apresentação, explicamos de maneira acessível os principais golpes virtuais, suas consequências legais e fornecemos dicas práticas de segurança digital, buscando contribuir para a formação cidadã dos participantes.

Ao final do evento, foi entregue um panfleto informativo elaborado pelos próprios alunos, contendo um resumo das orientações apresentadas na palestra, reforçando o compromisso com a informação e a prevenção.

O resultado do projeto foi bastante satisfatório, com ótima receptividade por parte do público presente e feedbacks positivos sobre a clareza e relevância do tema abordado.

7 CONCLUSÃO

Este projeto teve como objetivo principal investigar o estelionato virtual, com foco nos públicos mais vulneráveis, especialmente os jovens, buscando compreender as formas mais recorrentes deste crime, os mecanismos utilizados pelos golpistas virtuais e propor estratégias eficazes de prevenção por meio da educação digital. Ao longo do desenvolvimento, realizamos uma extensa pesquisa bibliográfica, análise de dados recentes e promovemos ações práticas de conscientização, como palestras educativas em instituições escolares, permitindo um contato direto com o público-alvo.

Uma das experiências mais marcantes vivenciadas pelo grupo foi a realização de palestras na Escola Estadual Nossa Senhora Auxiliadora, onde pudemos observar de perto o desconhecimento da maioria dos alunos em relação aos perigos reais presentes no ambiente digital. Enfrentamos desafios como a adaptação da linguagem técnica para uma comunicação acessível aos jovens, o que exigiu criatividade e sensibilidade para tornar o conteúdo relevante e compreensível. Esse processo nos mostrou a importância da empatia e da escuta ativa ao lidar com temas de impacto social.

Este projeto nos ensinou que a informação é a ferramenta mais poderosa para combater o estelionato virtual. Aprendemos sobre a importância da linguagem acessível, do trabalho em equipe e da responsabilidade social que envolve a produção e disseminação de conhecimento. Desenvolvemos habilidades fundamentais como planejamento de ações educativas, pesquisa científica aplicada, comunicação pública e trabalho colaborativo, que serão levadas para nossa trajetória acadêmica e profissional.

Para futuras ações, sugerimos a ampliação do projeto com a inclusão de oficinas práticas sobre o uso de ferramentas de segurança digital, a produção de vídeos educativos para redes sociais, e a

articulação com instituições públicas e privadas para promover campanhas de maior alcance. Acreditamos que, por meio de parcerias e continuidade, é possível fortalecer ainda mais a educação digital e reduzir significativamente os casos de estelionato virtual entre os jovens e demais grupos vulneráveis.

Assim, encerramos este trabalho com a convicção de que, embora o estelionato virtual seja um desafio complexo e em constante transformação, é possível enfrentá-lo com informação, prevenção e ação conjunta entre escola, socie Os resultados obtidos demonstraram que ações educativas simples, como rodas de conversa e distribuição de cartilhas, têm grande poder de alcance e impacto. Notamos maior engajamento dos alunos após as palestras, com relatos de jovens que compartilharam experiências de tentativas de golpes e que, a partir do conhecimento adquirido, sentiram-se mais preparados para se proteger. Por outro lado, percebemos a limitação de tempo e recursos para alcançar um público mais amplo, o que nos levou a refletir sobre a importância da continuidade e expansão dessas ações.

O impacto gerado foi significativo, especialmente na forma como os jovens passaram a enxergar a segurança digital. Um dos participantes nos relatou: *"Eu achava que essas coisas só aconteciam com gente mais velha, mas depois percebi que qualquer um pode cair nesses golpes, ainda mais quando a gente usa muito o celular."* Esse tipo de depoimento reforça a necessidade urgente de inserirmos a educação digital dade e poder público. O caminho é longo, mas cada passo dado rumo à conscientização digital é uma conquista importante na construção de uma internet mais segura para todos.

ANEXOS

REFERÊNCIAS

ALMEIDA, Gabriela Pinheiro. Crimes Cibernéticos: uma análise da legislação brasileira e perspectivas de prevenção. Dissertação (Mestrado em Direito) – Universidade de Brasília, 2018.

ALMEIDA, J. F. Crimes Cibernéticos e a Lei Carolina Dieckmann. São Paulo: Editora Atlas, 2021.

ALMEIDA, J. F. Proteção de Dados e Marco Civil da Internet: Uma Análise Crítica. São Paulo: Editora Atlas, 2021.

ATAÍDE, Amanda Albuquerque de. Crimes Virtuais: uma análise da impunidade e dos danos causados às vítimas. Maceió, 2017. Disponível em: http://www.faaiesa.edu.br/aluno/arquivos/tcc/tcc_amanda_ataide.pdf. Acesso em: 05 de mai. 2025.

BRASIL. Constituição da República Federativa do Brasil. Vade Mecum. 11. ed. São Paulo: Saraiva, 2017.

BRASIL. Lei nº 14.155, de 27 de maio de 2021. Altera o Código Penal e o Código de Processo Penal, para agravar a pena de crimes cometidos por meio eletrônico, digital ou simulado. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 27 maio 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2021/Lei/L14155.htm. Acesso em: 06 de mai. 2025.

CÂMARA DOS DEPUTADOS. Projeto de Lei nº 4554/2020. Modifica dispositivos do Código Penal, criando novas penas e medidas para crimes cometidos em ambiente digital. Câmara dos Deputados, Brasília, DF, 2020. Disponível em: https://www.camara.leg.br. Acesso em: 06 de mai. 2025.

COSTA, R. M. A Eficácia da Lei dos Crimes Cibernéticos no Brasil. Rio de Janeiro: Editora FGV, 2020.

COSTA, R. M. Marco Civil da Internet: Direitos e Deveres dos Usuários. Rio de Janeiro: Editora FGV, 2022.

CRUZ, Diego; RODRIGUES, Juliana. Crimes Cibernéticos e a Falsa Sensação de Impunidade. 2018. Disponível em: http://faef.revista.inf.br/imagens_arquivos/arquivos_destaque/iegWxiOtVJB1t5C_2019-2-28-16-36-0.pdf. Acesso em: 06 de mai. 2025.

FEITOZA, Luís Guilherme de Matos. Crimes Cibernéticos: o Estelionato Virtual. Brasília, 2012. Disponível em: https://egov.ufsc.br/portal/sites/default/files/crimesciberneticos_o_estelionato_virtual.pdf. Acesso em: 05 de mai. 2025.

FREITAS, Riany Alves de. Segurança Estelionato Digital. 2009. Disponível em: https://memoriadigital.mpmg.mp.br/wp-content/uploads/tainacan-items/4829/35770/14_Freitas.pdf . Acesso em: 05 de mai. 2025.

KSHETRI, N. International Perspectives on Cybercrime. Routledge, 2017.

LAKATOS, E. M.; MARCONI, M. DE A. Metodologia do trabalho científico. São Paulo: Atlas, 2014.

MAIA, T. S. F. Análise dos mecanismos de combate aos crimes cibernéticos no sistema penal brasileiro. Universidade Federal do Ceará. Faculdade de Direito, Curso de Direito, Fortaleza, 2017.

MARCO CIVIL DA INTERNET. Disponível em: http://www.planalto.gov.br/ccivil_ 03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 05 de mai. 2025.

MAUES, Gustavo Brandão Koury et. al. Crimes Virtuais: uma análise sobre a adequação da legislação penal brasileira. 2018. Disponível em: https://www.unirios.edu.br/revistarios/media/revistas/2018/18/crimes_virtuais.pdf . Acesso em: 05 de mai. 2025.

MENDES, A. L. O Marco Civil da Internet e Seus Impactos na Proteção de Dados. Brasília: Editora da Câmara dos Deputados, 2020.

OLIVEIRA, P. R. Educação Digital e Proteção de Dados na Era da Informação. Porto Alegre: Editora PUC, 2022.

REGIS, André Tavares. Crimes Contra a Honra na Internet: Dificuldade na Apuração dos Fatos. João Pessoa, 2011.

RIBEIRO, L. A. Privacidade e Segurança na Era Digital: O Caso Carolina Dieckmann. Brasília: Editora da Câmara dos Deputados, 2019.

SANTOS, C. L. Cibercrimes e a proteção penal no Brasil: desafios da era digital. São Paulo: Revista dos Tribunais, 2020.

SANTOS, Liara Ruff dos et. al. Os crimes cibernéticos e o direito a segurança jurídica: uma análise da legislação vigente no cenário brasileiro contemporâneo. Santa Maria, 2017. Disponível em: http://coral.ufsm.br/congressodireito/anais/2017 /7-7.pdf. Acesso em: 05 de mai. 2025.

SILVA, T. R. Privacidade e Segurança na Era Digital: Desafios do Marco Civil. Belo Horizonte: Editora UFMG, 2021.

SOUZA, Júlio Cesar. Investigação Criminal Pela Polícia Militar e Sua Inconstitucionalidade. 2012.

SOUZA, P. R. Educação Digital e Conscientização em Segurança da Informação. Porto Alegre: Editora PUC, 2022.

SPINIELI, André Luiz Pereira. Crimes informáticos: comentários ao projeto de Lei n° 5.555/2013. Brasília, 2018. Disponível em: http://www.mpf.mp.br/atuacaotematica/ccr2/publicacoes/coletaneas-de-artigos/coletanea_de_artigos_crimes_ciberneticos. Acesso em: 05 de mai. 2025.

VASCONCELLOS, M. R. O marco civil da internet e a cooperação internacional no combate aos crimes cibernéticos. Belo Horizonte: Fórum, 2020.

WENDT, Emerson e NOGUEIRA JORGE, Higor Vinicius Nogueira. Editora Braspot. Crimes Cibernéticos: Ameaças e Procedimentos de Investigação – 2º Edição. 2017. crimes virtuais, uso de dados roubados e afins.