CENTRO UNIVERSITÁRIO DE GOIÁS – UNIGOIÁS
PRÓ-REITORIA DE ENSINO PRESENCIAL – PROEP
SUPERVISÃO DA ÁREA DE PESQUISA CIENTÍFICA - SAPC
CURSO DE DIREITO

ATAQUES VIRTUAIS: UMA EXPLORAÇÃO DOS DELITOS CIBERNÉTICOS E SEU IMPACTO NA PRIVACIDADE ONLINE

CINTHIA ELLEN MARQUES VIEIRA
ORIENTADORA: CASSIRA LOURDES DE ALCÂNTARA DIAS RAMOS JUBÉ

GOIÂNIA
Dezembro/2024

CINTHIA ELLEN MARQUES VIEIRA

ATAQUES VIRTUAIS: UMA EXPLORAÇÃO DOS DELITOS CIBERNÉTICOS E SEU IMPACTO NA PRIVACIDADE ONLINE

Trabalho final de curso apresentando e julgado como requisito para a obtenção do grau de bacharelado no curso de Direito do Centro Universitário de Goiás – UNIGOIÁS na data de 01/10/2024.

_____
Ma. Cassira Lourdes de Alcântara Dias Ramos Jubé (Orientador/a)
Centro Universitário de Goiás - UNIGOIAS

_____
Me. Allan Kardec Cabral Jr (Examinador/a)
Centro Universitário de Goiás - UNIGOIAS

_____
Esp. Sávio César Santana (Examinador/a)
Centro Universitário de Goiás - UNIGOIAS

ATAQUES VIRTUAIS: UMA EXPLORAÇÃO DOS DELITOS CIBERNÉTICOS E SEU IMPACTO NA PRIVACIDADE ONLINE

Cinthia Ellen Marques Vieira[1]
Cassira Lourdes de Alcântara Dias Ramos Jubé[2]

Resumo: Este trabalho aborda os crimes cibernéticos e seu impacto na privacidade online, destacando a evolução desses delitos e a eficácia da legislação brasileira no combate a essas ameaças. O problema que motivou a pesquisa reside na crescente incidência de crimes virtuais e nas lacunas existentes nas leis que regulam a proteção da privacidade digital. Os objetivos são analisar as principais espécies de crimes cibernéticos, avaliar a efetividade das legislações como a Lei Geral de Proteção de Dados (LGPD) e propor melhorias nas políticas de cibersegurança. A metodologia utilizada inclui análise documental e revisão bibliográfica, com foco em fontes acadêmicas e legais relevantes. Os principais resultados indicam que, embora existam leis que visam proteger a privacidade, estas são insuficientes diante da complexidade e evolução dos crimes virtuais. Conclui-se que é necessário um fortalecimento das normas jurídicas, juntamente com um investimento em educação e conscientização digital, para garantir a segurança e a privacidade dos cidadãos no ambiente digital.

Palavras-chave: segurança online. delitos virtuais. legislação digital. proteção de dados pessoais. cibersegurança.

VIRTUAL ATTACKS: AN EXPLORATION OF CYBER CRIMES AND THEIR IMPACT ON ONLINE PRIVACY

Abstract: *This work addresses cybercrimes and their impact on online privacy, highlighting the evolution of these crimes and the effectiveness of Brazilian legislation in combating these threats. The problem that motivated the research lies in the growing incidence of virtual crimes and the gaps in the laws that regulate the protection of digital privacy. The objectives are to analyze the main types of cybercrime, evaluate the effectiveness of legislation such as the General Data Protection Law (LGPD) and propose improvements to cybersecurity policies. The methodology used includes document analysis and bibliographic review, focusing on relevant academic and legal sources. The main results indicate that, although there are laws that aim to protect privacy, these are insufficient given the complexity and evolution of virtual crimes. It is concluded that it is necessary to strengthen legal standards, together with an investment in education and digital awareness, to guarantee the security and privacy of citizens in the digital environment.*

KEYWORDS: *online security. virtual crimes. digital legislation. protection of personal data. cybersecurity.*

INTRODUÇÃO

A crescente dependência das tecnologias digitais trouxe consigo um aumento significativo nos crimes cibernéticos, afetando diretamente a privacidade online. Esses ataques virtuais representam uma ameaça tanto para indivíduos quanto para organizações, exigindo respostas jurídicas e técnicas cada vez mais eficazes. Este trabalho tem como foco analisar os

[1] Discente do curso de Direito do Centro Universitário de Goiás – UNIGOIÁS. Lattes: https://lattes.cnpq.br/8281700834865309. Orcid: 0009000507305354. E-mail: cinthiamarquesvieira@gmail.com.
[2] Mestre em Direitos Humanos pelo Programa Interdisciplinar de Mestrado em Direitos Humanos da Universidade Federal de Goiás - Núcleo de Direitos Humanos. Especialista em Direitos Humanos (2002) e Docência Universitária (2003). Possui graduação em Direito pela Pontifícia Universidade Católica de Goiás (2001). Atualmente é professora mestre do Centro Universitário de Goiás - Uni-Anhanguera, atuando principalmente nos seguintes temas: Direitos Humanos, Cidadania, Direito Penal e Processual Penal, Direito Internacional, Segurança Pública e Prevenção. Advogada inscrita na Ordem dos Advogados de Goiás, desde 2005, atuando nos ramos de direito público e privado. Lattes: http://lattes.cnpq.br/6792979547523586. Orcid: 6792979547523586. E-mail: cassiratcc@gmail.com.

delitos cibernéticos e seu impacto na privacidade online, explorando os principais tipos de crimes virtuais, suas implicações legais e as lacunas na proteção de dados pessoais. O tema será delimitado ao contexto brasileiro, com ênfase nas legislações aplicáveis e nos desafios que ainda existem para garantir a segurança e a privacidade na era digital.

A pesquisa tem como objetivo principal compreender a dinâmica dos crimes cibernéticos e suas diversas manifestações, além de identificar como esses crimes afetam a privacidade online dos usuários. Busca-se ainda investigar as lacunas existentes na legislação brasileira, propor possíveis aprimoramentos nas normas jurídicas e sugerir soluções práticas para combater as ameaças cibernéticas de forma mais eficaz. A pesquisa também pretende sensibilizar sobre a importância da conscientização digital como mecanismo preventivo.

A escolha do tema foi motivada pela crescente preocupação com a segurança no ambiente digital e o aumento expressivo de crimes cibernéticos nos últimos anos. O uso intensivo de tecnologias e a massiva circulação de dados pessoais na internet colocam em risco a privacidade dos indivíduos, tornando urgente a discussão sobre mecanismos de proteção eficazes. Este estudo se faz relevante socialmente, pois visa contribuir para a melhoria das práticas de segurança digital e para o fortalecimento do arcabouço jurídico no Brasil, promovendo maior proteção para os cidadãos.

A relevância social da pesquisa está relacionada à necessidade de proteger os direitos fundamentais dos indivíduos em um cenário onde a privacidade online é frequentemente violada. O estudo deste tema é importante para garantir que as legislações e políticas públicas acompanhem a evolução tecnológica, garantindo que os cidadãos possam navegar na internet com segurança. Além disso, a busca por soluções jurídicas mais eficazes pode contribuir para a criação de um ambiente digital mais seguro e confiável para todos.

A pesquisa inicia com uma análise teórica sobre os crimes cibernéticos, suas origens e evolução, destacando como a tecnologia digital permitiu o surgimento de novas formas de criminalidade. No primeiro capítulo, é discutido o conceito de crimes virtuais e a teoria geral do crime, aplicando-a ao ambiente digital para esclarecer a tipicidade, ilicitude e culpabilidade nesses delitos. O segundo capítulo explora as principais espécies de crimes cibernéticos, como fraudes financeiras, roubo de dados e engenharia social, detalhando suas características e os impactos que causam às vítimas.

No terceiro capítulo, o foco está no impacto dos crimes cibernéticos na privacidade online, destacando como as violações de dados pessoais afetam a segurança e a confiança dos usuários na internet. O quarto capítulo aborda a legislação e regulação no Brasil, analisando o papel da Lei Geral de Proteção de Dados (LGPD) e da Lei Carolina Dieckmann na proteção

contra crimes virtuais. O estudo finaliza com o quinto capítulo, onde são discutidas estratégias de prevenção e propostas de aprimoramento da legislação para enfrentar os desafios impostos pelos delitos cibernéticos, além de medidas práticas para proteger a privacidade no ambiente digital.

MATERIAIS E MÉTODOS

Este trabalho desenvolve uma abordagem qualitativa, buscando compreender e explorar os crimes cibernéticos e seu impacto na privacidade online, por meio da análise teórica e revisão de literatura. A pesquisa é caracterizada como exploratória, uma vez que pretende aprofundar o entendimento sobre os desafios impostos pelos delitos virtuais, com foco nas brechas e lacunas da legislação brasileira, assim como na evolução desses crimes ao longo do tempo.

Para conduzir essa pesquisa, optou-se pela análise documental e revisão bibliográfica, utilizando fontes como livros, artigos científicos, leis brasileiras, jurisprudência e dados de especialistas na área de direito digital e segurança cibernética. As referências são selecionadas de forma a oferecer uma visão abrangente e atualizada sobre o tema, incluindo discussões sobre a Lei Geral de Proteção de Dados (LGPD) e a Lei Carolina Dieckmann.

O recorte temporal concentra-se nos últimos 15 anos, período em que as legislações específicas para o combate aos crimes cibernéticos no Brasil ganham relevância, especialmente com a evolução da internet e o aumento da digitalização de dados pessoais. Já o recorte espacial abrange o cenário jurídico brasileiro, uma vez que a pesquisa visa avaliar o impacto e a efetividade das leis nacionais na proteção contra delitos cibernéticos.

A técnica de análise de dados inclui a interpretação crítica dos documentos e textos acadêmicos revisados, buscando identificar padrões, inconsistências e contribuições teóricas sobre o tema dos crimes virtuais. As discussões resultantes dessa análise proporcionam embasamento para as conclusões apresentadas ao longo do trabalho, que tem como objetivo contribuir para o aprimoramento das políticas de cibersegurança no Brasil.

1. ASPECTOS GERAIS DOS CRIMES CIBERNÉTICOS

1.1 DEFINIÇÃO DOS CRIMES CIBERNÉTICOS

Analisando o cenário atual, os crimes cibernéticos são um problema que se alastra no meio social, crime esse, que é alimentado pela tecnologia da informação que penetram as vulnerabilidades dos sistemas e redes. Ainda mais, a tecnologia veio com a função de facilitar

a vida das pessoas, trazendo modernização na comunicação, acesso à informação e eficiência, porém, os criminosos utilizam-se dessa tecnologia cibernética para o cometimento de crimes no âmbito virtual.

É importante ressaltar que, antes de tratar especificadamente dos crimes cibernéticos, é fundamental, portanto, analisar a teoria geral do crime, pois oferece a base necessária para identificar os elementos que constituem uma conduta criminosa, facilitando a análise das particularidades do ambiente virtual e responsabilizar seus autores. Conforme argumenta Araújo (2021), a teoria do crime oferece ferramentas essenciais para interpretação de delitos em qualquer contexto, inclusive no âmbito cibernético. Dentre diversos conceitos utilizados para definir o crime, existem ideias básicas que são comuns a todos, uma dessas ideias é que causa evento danoso a sociedade como um todo, e que esse evento danoso deve responsabilizar apenas o sujeito ativo que é o autor do fato.

Um dos principais conceitos para crime é o analítico onde pode-se apreciar o conceito de crime sob três aspectos distintos a depender da teoria a ser adotada e a mais aceita é a teoria tripartida que cujos seus elementos são tipicidade, ilicitude e culpabilidade. Como afirma Araújo (2021, p. 333) de forma objetiva, a tipicidade é a relação de (perfeita) adequação da conduta humana ao tipo. Ou seja, a tipicidade ocorre quando a conduta do agente de enquadra no tipo que foi descrito, como exemplo art. 154-A, do Código Penal, que está descrito sobre a invasão de dispositivo informático, isto é, o tipo está descrito e a conduta do agente é a tipicidade. Além da tipicidade, a conduta deve ser ilícita, ou seja, contrária ao direito, salvo se houver causas de exclusão como legítima defesa ou exercício regular de um direito Araújo, (2021). No ambiente cibernético, a ilicitude se manifesta quando ações, como a violação de dispositivos, violam direitos como a privacidade. A culpabilidade, por sua vez, refere-se à reprovação da conduta, analisando se o agente tinha capacidade de entender o caráter ilícito do ato e agir de forma diferente. Nos crimes cibernéticos, também é necessário verificar se o autor tinha consciência da ilicitude da ação.

De acordo com Wendt e Jorge (2021), os crimes cibernéticos são definidos como uma ampla gama de atividades criminosas que envolve o mau uso da tecnologia para o cometimento de crimes com a finalidade de alcançar os seus objetivos. Esses crimes virtuais englobam diversas atividades criminosas, como a invasão de sistemas de computador, roubos de informações pessoais e financeiras e fraudes online. Uma das características do cometimento desse crime é a possiblidade de proceder atos transnacional e a capacidade de agirem anonimamente, cruzando fronteiras sem deixar rastros.

Os crimes cibernéticos não se limitam apenas à invasão de sistemas de computador ou roubo de informações pessoais. Eles abrangem uma ampla gama de atividades criminosas que exploram as vulnerabilidades da tecnologia da informação para alcançar objetos ilícitos. Isso pode incluir ataques de *phishing*,[3] onde os criminosos tentam enganar os usuários a divulgar informações confidenciais, e o uso de malware para interromper sistemas ou roubar dados e pode se manifestar de várias formas, incluindo vírus, trojans. (Furlaneto, 2023)

Um caso notório e de fundamental importância para a criação da Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, foi o incidente envolvendo a atriz que teve o seu computador invadido e fotos íntimas roubadas por hackers. Esse acontecimento gerou grande repercussão na mídia e destacou a vulnerabilidade das informações na era digital. O caso da atriz serviu como um alerta poderoso sobre a necessidade de proteger a privacidade online e de fortalecer as leis de cibersegurança no Brasil, contribuindo, assim, para o endurecimento das leis de proteção digital.

Além dos ataques diretos a sistemas de computadores, os crimes cibernéticos envolvem também métodos mais surtis, como ransomware, onde os arquivos são criptografados e é exigido um valor para ser liberados. O papel crucial que a evolução tecnológica desempenha na sociedade é fundamental para o progresso humano, e desenvolvimento social. À medida que a sociedade se torna cada vez mais dependente da tecnologia, inovações surgem como a inteligência artificial, podendo, assim, os criminosos adaptarem suas táticas para explorar novas vulnerabilidades e possibilidades de ataques. Esses crimes têm um impacto significativo na economia global, causando perdas financeiras substanciais para empresas e indivíduos, levando a consequências financeiras ao longo prazo. Além disso, os custos associados à prevenção e mitigação de ataques cibernéticos também são significativos.

Os crimes cibernéticos não se limitam a ataques direitos a sistemas de computadores, quase sempre envolvem também engenharia social. Wendt e Jorge (2021, p. 41) define engenharia social como: “Um conjunto de técnicas destinadas a ludibriar a vítima, de forma que ela acredite nas informações prestadas e se convença a fornecer dados pessoais nos quais o criminoso tenha interesse ou a executar alguma tarefa e/ou aplicativo”.

Logo, os criminosos atingem pessoas com pouco conhecimento no mundo virtual, onde as vítimas podem ter o seu computador infectado com vírus, podendo ocorrer além do computador, por telefone. Vale destacar que os criminosos frequentemente utilizam técnicas criativas e de persuasão para enganar as vítimas e obter informações importantes. Nestes

[3] O termo *phishing* é originado da palavra inglesa *fishing*, que significa pescar, ou seja, é a conduta daquele que pesa informações sobre o usuário de computador.

termos, a engenharia social passar a afetar tanto o físico como psicológico. No físico, exploram o local de trabalho, vasculham lixeiras, e por telefone se passam por outra pessoa. No psicológico, exploram o lado sentimental das pessoas. (Popper e Brignoli, 2017)

A natureza transnacional dos crimes cibernéticos apresenta desafios significativos para a aplicação da lei e a cooperação internacional. As leis e regulamentações relacionadas à segurança cibernéticas variam de país a país, dificultando a persecução de criminosos que operam além das fronteiras nacionais. Inclusive, questões de jurisdição e jurisprudência complicam ainda mais os esforços para responsabilizar os culpados e garantir a justiça para as vítimas. (Interpol)

Assim, os crimes ligados a tecnologia são uma ameaça que está em constante evolução global e cada vez torna-se mais dependentes da tecnologia, é de grande importância que a sociedade esteja vigilante e adotem medidas para proteger seus sistemas contra as ameaças digitais.

1.2 A EVOLUÇÃO DOS CRIMES CIBERNÉTICOS

Os crimes cibernéticos têm evoluído rapidamente em resposta ao avanço da tecnologia e às mudanças nas táticas criminosas. Explorando a vulnerabilidade dos usuários, os criminosos têm refinado suas estratégias ao utilizar informações no meio público. A expansão dos crimes no mundo digital foi acompanhada por uma grande sofisticação nas técnicas utilizadas, como o desenvolvimento de avançadas técnicas de engenharia social, que exploram a falta de conhecimento dos usuários para acessar informações confidenciais. Esta evolução na técnica de engenharia social foi um divisor de águas na transformação dos crimes cibernéticos.

De acordo com Agência Câmera de Notícias (2006), os primeiros crimes relacionados à informática foram praticados na década de 1960, nos Estados Unidos. Na época, começaram a aparecer na imprensa e na literatura científica norte-americana os primeiros casos de uso de computadores para cometer delitos como sabotagens e espionagem. Somente na década seguinte, foram iniciados estudos sistemáticos e científicos sobre o tema. A partir de 1980, as ações criminosas intensificaram-se, envolvendo principalmente manipulação de dados bancários, pirataria de programas de computador, abusos nas telecomunicações e pornografia infantil.

A contínua sofisticação e organização dos criminosos tornam difícil rastreá-los e responsabilizá-los, exigindo respostas eficazes e colaboração internacional em segurança cibernética. Os grupos exploram vulnerabilidades em sistemas digitais para atividades como roubo de dados, fraude financeira e extorsão. A diversificação dos tipos de crimes também é

uma marca diferenciada da evolução dos crimes cibernéticos, incluindo novas ameaças como a disseminação de deepfakes, que desafiam a segurança cibernética e exigem respostas rápidas das autoridades. (Siqueira, 2019)

Os criminosos estão cada vez mais adaptando suas táticas para explorar as mais recentes tecnologias, incluindo o uso de inteligência artificial para automatizar ataques, a exploração de dispositivos vulneráveis e o uso de engenharia social cada vez mais sofisticada para manipular as vítimas. Portanto, a evolução dos crimes digitais juntamente com a crescente sofisticação dos criminosos torna difícil rastrear e responsabilizar os culpados. Apesar dos esforços para aumentar a segurança cibernética, muitos indivíduos e organizações ainda são negligentes em suas práticas de segurança, deixando vulnerabilidades que os criminosos estão prontos para explorar.

Os crimes cibernéticos não afetam apenas indivíduos e empresas, mas também têm um impacto significativo na segurança nacional e na economia global. Ataques cibernéticos direcionados a infraestruturas críticas, como redes elétricas e sistemas financeiros, podem causar danos graves e exigem medidas preventivas robustas. A implementação de políticas de segurança cibernética e ações preventivas dos usuários para as melhores práticas no âmbito da rede, para minimizar o risco de ataques, para garantir a proteção contra essas ameaças. (Canongia e Junior, 2009)

A falta de cooperação internacional e a divergência nas leis cibernéticas entre os países dificultam a investigação e a punição dos criminosos cibernéticos. É essencial desenvolver tratados internacionais que estabeleçam diretrizes claras para a responsabilização desses criminosos e promovam a cooperação global em segurança cibernética. A capacitação contínua das forças policiais e dos órgãos reguladores é crucial para manter a eficácia na detecção e prevenção de crimes cibernéticos. (Interpol)

A crescente incidência de crimes cibernéticos também levanta questões éticas sobre a privacidade e a vigilância digital. A balança entre segurança e privacidade tornou-se um ponto crítico de debate público, destacando a necessidade de políticas que equilibrem esses interesses de maneira equitativa. A proteção dos direitos individuais deve ser uma prioridade nas estratégias de segurança cibernética, garantindo que as medidas adotadas respeitem os direitos fundamentais dos cidadãos.

Portanto, o avanço dos crimes cibernéticos representa um desafio significativo para a segurança global, exigindo uma resposta coordenada e abrangente. A adaptação contínua das leis e regulamentos, o fortalecimento da educação em segurança cibernética e a promoção da

cooperação internacional são essenciais para proteger indivíduos, empresas e governos contra as ameaças emergentes no cenário digital. (Interpol)

1.3 O MEIO AMBIENTE DIGITAL E AS TUTELAS DOS DIREITOS FUNDAMENTAIS

Os crimes cometidos por intermédio da informática em ambiente de rede[4], tem desafiado a aplicação e proteção dos direitos fundamentais no âmbito virtual. Isso abrange inúmeras transformações tecnológicas, ocasionado novas possibilidades de comunicação, e assim surgiu os novos desafios de proteção a privacidade, e liberdade de expressão e outros direitos fundamentais. Trazendo à tona como o meio ambiente digital influencia e envolve os direitos fundamentais, mostrando assim suas complexidades no que envolve assegurar sua proteção adequada.

Os direitos fundamentais são direitos inalienáveis que garantem a proteção da liberdade, igualdade e dignidade de todos os indivíduos. (Oliveira *et al*., 2024). No meio digital, esses direitos envolve a privacidade dos indivíduos, liberdade de expressão, e a principal de todas o acesso a informação. É de fundamental importância entender a forma que esses direitos são aplicados no ambiente digital, onde as novas tecnologias podem afetar a sua aplicação, onde a internet passa além na noção de lugar, como Fiorillo e Conte (2016, p. 13) comenta:

> A internet permite conectar computadores de qualquer parte do mundo sempre que estes se encontram na rede, através de sistemas de comunicação que interagem por um conjunto de regras conhecidas como Protocolo. A internet não se apresenta, nessa esteira, como entidade física ou tangível, mas configura uma rede de redes interligadas. Com o advento da internet e, com ela, do ciberespaço, a concepção clássica de território transfigurou-se, uma vez que esta possibilidade o tráfego rápido e eficiente de informações, bem como a interação num espaço desconhece os limites impostos por fronteiras.

Os direitos fundamentais evoluíram para abranger os novos desafios e necessidade que surgiram com o avanço da tecnologia, era focado incialmente em proteger a disseminação de desinformação. O reconhecimento desses desafios impulsionou a criação de leis e regulamentos que visam proteger a privacidade e a segurança dos dados pessoais. (Oliveira *et al*., 2024)

O meio ambiente digital engloba o conjunto de dispositivos, redes e serviços que compõem o espaço digital. Esse ambiente é caracterizado pela interconexão de dispositivos, processamento e compartilhamento de dados pessoais e não pessoais. A interação no meio ambiente digital ocorre através da internet, lugar onde conecta os indivíduos em todo o mundo. Neste sentido, Fiorillo e Conte (2016, p. 16) elucida sobre o meio ambiente digital e a relação de direitos e deveres:

[4] O termo *ambiente de rede*, é o espaço virtual onde os dispositivos conectados à internet ou a uma interação de internet, permitindo o acesso remoto a informações e a comunicação global em tempo real.

> O meio ambiente digital, por via de consequência, fixa no âmbito de nosso direito positivo os deveres, direitos, obrigações e regime de responsabilidade inerentes à manifestação de pensamento, criação, expressão e informação realizados pela pessoa humana coma ajuda de computadores (art. 220 da Constituição Federal) dentro do pleno exercício dos direitos culturais assegurados a brasileiros e estrangeiros residente no País (arts. 215 e 5º da Constituição Federal) orientado pelos princípios fundamentais da Constituição Federal (arts. 1º a 4º da Constituição Federal).

Trata de um dos mais importantes direitos quando se refere em manifestação de pensamentos, e sua expressão. Onde as novas tecnologias de informação afetam o lazer e ao entretenimento. O direito de Jogar, de passar tempo no Facebook, está inserido ao direito ao lazer e ao entretenimento que se encontra no art. 6º da Constituição Federal: "São direitos sociais a educação, a saúde, o trabalho, o lazer, a segurança, a previdência social, a proteção à maternidade e à infância, a assistência aos desamparados, na forma desta Constituição."

A proteção da privacidade e dos dados pessoais é crucial no ambiente digital, onde a coleta e análise de informações podem comprometer a liberdade e segurança dos indivíduos. De forma semelhante, a liberdade de expressão e acesso à informação são pilares fundamentais da democracia, e são frequentemente desafiados por práticas com censura online e manipulação de conteúdo. A interação entre esses direitos é complexa, e requer um equilíbrio delicado entra a proteção individual e a liberdade coletiva dos indivíduos. (Fiorillo, 2016).

O meio ambiente digital apresenta novos desafios para a proteção dos direitos fundamentais, incluindo vulnerabilidades tecnológicas e práticas criminosas como fraudes. Esses crimes não apenas ameaçam à integridade das pessoas como também desafia a eficácia das leis existentes. A proteção dos direitos fundamentais no meio digital depende da implementação de legislação abrangente e regulamentação adequadas. A Lei Geral de Proteção de Dados, é um exemplo de normativa que visa proteger os dados pessoais dos indivíduos.

No entanto, a legislação se diferencia em cada país, e assim cria desafios para a proteção dos direitos fundamentais. Neste contexto, o Brasil aceitou o convite de participação da Convenção de Budapeste, um tratado internacional que busca fortalecer a cooperação entre países no combate aos crimes cibernéticos. Essa adesão representa um avanço importante para aprimorar a proteção jurídica no Brasil em relação aos crimes no ambiente virtual. (Rosa, *et al.*, 2024).

Para o enfrentamento quanto aos desafios que surgem na proteção dos direitos fundamentais no meio ambiente requer-se uma abordagem colaborativa mais abrangente e proativa, propostas para fortalecer a proteção que incluem a implementação de legislação mais rigorosa, o fortalecimento da aplicação da lei e o desenvolvimento de tecnologias que protejam a privacidade e a segurança dos indivíduos online. A educação contínua quanto ao meio digital

é essencial para enfrentar os desafios e garantir que os direitos fundamentais sejam protegidos de maneira eficaz.

2. ESPÉCIES DE CRIMES CIBERNÉTICOS

2.1. FRAUDES E CRIMES FINANCEIROS

Com o crescimento e avanço da internet, embora seja uma ferramenta destinada a conectar pessoas e facilitar as atividades diárias, também abriu portas para o cometimento de crimes no âmbito virtual, envolvendo o uso de sistemas informáticos. Entre os crimes comuns estão os crimes de pornografia infantil, *ciberbullying*[5], financeiros. As fraudes e crimes financeiros estão entre os que mais ocorrem atualmente.

A fraude pode ser caracterizada como "qualquer ato ardiloso, enganoso, de má-fé, com o intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro", conforme o dicionário. Pode-se observar que fraude pode ocorrer entre diversos ambiente, incluindo ambiente virtual, chamando assim de fraude eletrônica. A natureza desses crimes digitais permite que os perpetradores utilizem uma variedade de técnicas para enganar e explorar suas vítimas de maneira mais eficaz e menos rastreável. (Souza, 2023)

Entre as múltiplas formas e modalidades dos crimes de fraudes, observa-se uma variedade de práticas que exploram as vulnerabilidades do ambiente digital para obter ganho ilícitos. Um exemplo significativo é o *phishing*, uma técnica de engenharia social onde os criminosos se disfarçam como instituições confiáveis para obter informações pessoais e financeiras das vítimas. Esse método geralmente é realizado por meio de e-mails ou mensagens fraudulentas que simulam comunicações legítimas, enganando os usuários a fornecer dados confidenciais.

Além do phishing, os golpes de investimento são especificamente uma forma complexa de fraude financeira. Esses golpes envolvem a criação de esquemas fraudulentos que prometem retornos financeiros elevados com baixo risco, atraindo investidores com a promessa de lucros rápidos. No entanto, esses esquemas geralmente resultam em grandes perdas para as vítimas, uma vez que o investimento é desviado para os criminosos. (Souza, 2023)

Outro exemplo são as fraudes em cartões de crédito, que envolvem a obtenção e uso não autorizado das informações de cartões para realizar transações fraudulentas. Essas fraudes podem ser perpetradas por meio de malware, ataques de phishing ou o roubo físico de cartões,

[5] O termo "*ciberbullying"*, é utilizado para explicar quando o indivíduo recorre à tecnologia para intimidar alguém, humilhar, ameaçar.

levando a prejuízos significativos para os titulares e para as instituições financeiras. (Souza, 2023)

A dinâmica desses crimes financeiros é acentuada pela constante evolução das técnicas empregadas pelos criminosos e pela sofisticação dos métodos utilizados. Os criminosos cibernéticos estão continuamente desenvolvendo novas estratégias para explorar falhas de segurança e enganar suas vítimas, (Souza, 2023). Dessa forma, a necessidade de estratégias robustas e adaptativas para prevenir e combater fraudes eletrônicas torna-se cada vez mais urgente.

Portanto, a análise das fraudes e crimes financeiros no ambiente digital não apenas revela a complexidade e a diversidade das práticas criminosas, mas também sublinha a importância de uma vigilância contínua e de políticas de segurança cibernética eficazes. A proteção da integridade financeira e da segurança dos usuários exige uma abordagem abrangente que inclua a educação sobre segurança digital, o desenvolvimento de tecnologias avançadas de proteção e a implementação de medidas regulatórias rigorosas para mitigar o impacto desses crimes. (Souza, 2023)

2.2. ROUBO DE DADOS

O roubo de dados é uma das formas mais prevalentes e prejudiciais de crime cibernético, especialmente em um mundo cada vez mais digitalizado, onde dados pessoais e sensíveis são amplamente armazenados em plataformas online. Este tipo de crime envolve a obtenção não autorizada de informações privadas, que podem incluir desde dados financeiros, como números de cartões de crédito, até informações pessoais e confidenciais, como dados médicos ou credenciais de acesso a sistemas corporativos. (Silveira e Santos, 2024)

O roubo de dados pode ocorrer de diversas formas, sendo frequentemente facilitado por ataques de malware ou, ainda, por meio de invasões diretas a sistemas informatizados que contêm essas informações. Ataques de ransomware também são cada vez mais comuns, onde criminosos sequestram dados e exigem pagamento para a sua devolução. Outra forma envolve a utilização de keyloggers, programas maliciosos que registram tudo o que o usuário digita, incluindo senhas e outras informações sensíveis. (Silveira e Santos, 2024)

A motivação por trás do roubo de dados é variada. Em muitos casos, as informações roubadas são utilizadas para realizar fraudes financeiras, como a abertura de contas bancárias em nome da vítima ou o uso não autorizado de cartões de crédito. Em outros cenários, os dados

podem ser vendidos no mercado negro, onde informações pessoais têm um alto valor, ou utilizados para extorquir as vítimas ou as empresas que detêm os dados roubados.

Estudos realizados por Silveira e Santos apontam que o impacto do roubo de dados pode ser devastador tanto para indivíduos quanto para corporações. Indivíduos podem enfrentar desde perdas financeiras até danos à sua reputação, especialmente em casos onde suas identidades são utilizadas para fins fraudulentos. No caso de empresas, a exposição de dados sensíveis pode resultar em multas significativas, perda de confiança por parte de clientes e parceiros, além de consequências legais, especialmente em países onde legislações como o GDPR na Europa e a LGPD no Brasil impõem pesadas sanções para o descumprimento das normas de proteção de dados.

Conforme estudiosos como Silveira e Santos (2024) apontam, o roubo de dados não se limita apenas ao ambiente financeiro. Dados sensíveis de caráter pessoal, como endereços, números de telefone e até preferências de consumo, também são alvos valiosos. A crescente utilização de dispositivos conectados à Internet das Coisas (IoT) amplia ainda mais o campo de vulnerabilidade, já que esses aparelhos geralmente têm níveis de segurança inferiores, facilitando o acesso não autorizado.

O combate ao roubo de dados requer medidas de segurança robustas, que vão desde a implementação de políticas de proteção de dados nas empresas até a conscientização dos usuários sobre boas práticas de segurança cibernética. Ferramentas como criptografia de dados, autenticação de dois fatores e firewalls avançados são essenciais para prevenir tais crimes. Ademais, é fundamental que as empresas invistam em treinamento contínuo de seus funcionários para evitar que ataques como phishing comprometam sistemas inteiros.

Além das medidas preventivas, a legislação desempenha um papel crucial na proteção contra o roubo de dados. Leis como a Lei Geral de Proteção de Dados (LGPD) no Brasil estabelecem diretrizes claras para o tratamento e proteção de dados pessoais, exigindo das empresas uma postura ativa na preservação da privacidade e da integridade das informações que gerenciam. Contudo, o desafio da aplicação dessa legislação em um ambiente digital em constante mudança permanece significativo. (Souza, 2023)

Portanto, para combater eficazmente essas ameaças, é crucial adotar uma abordagem multifacetada que inclua tanto medidas comportamentais quanto tecnológicas. A conscientização desempenha um papel fundamental; portanto, é essencial promover o treinamento contínuo para funcionários, garantindo que todos estejam cientes das técnicas de engenharia social e saibam como reconhecer sinais de alerta.

2.3. ENGENHARIA SOCIAL

A engenharia social é a prática amplamente adotada por criminosos cibernéticos para manipular indivíduos, visando obter informações confidenciais e acesso a sistemas protegidos. Diferente dos métodos tradicionais, a engenharia social se baseia na manipulação do comportamento humano, ao explorar vulnerabilidades emocionais, como a confiança, medo, os engenheiros sociais conseguem contornar até mesmo as mais avançadas barreiras de segurança. Essa técnica de manipulação envolve induzir as vítimas a revelar informações confidenciais ou realizar ações prejudiciais à segurança. Esses ataques não precisam de brechas tecnológicas, mas sim de uma abordagem tecnológica, muitas vezes manipulando as emoções e a confiança das pessoas. (Veridian, 2023)

Enquanto o *hacking* tradicional se concentra em explorar falhas em softwares e sistemas para obter acesso não autorizado, a engenharia social manipula a confiança humana para alcançar seus objetivos. Esses métodos não exigem conhecimento técnico profundo, mas são eficazes porque exploram fraquezas comportamentais. O objetivo ao utilizar essa engenharia pode variar, desde o roubo de informações pessoais e financeiras até o acesso a sistemas corporativos ou governamentais. Esses ataques podem resultar em prejuízos financeiros significativos, comprometer dados sensíveis e até mesmo causar danos irreparáveis à reputação das vítimas. (Veridian, 2023)

Diversos métodos são empregados para ludibriar vítimas, obter informações e acessos. Entre os mais comuns, destacam-se: pretexting, segundo Veridian (2023) consiste em criar uma história ou em cenário falso para obter informações de uma pessoa. O manipulador se passa por uma pessoa ou instituição confiável para enganar a vítima e obter acesso a informações valiosas. Geralmente, estudam suas vítimas detalhadamente, utilizando informações pessoais para criar cenários convincentes, para a obtenção de lucro ou espionagem.

Os ataques de engenharia social podem ter consequências graves tanto para indivíduos quanto para empresas. Além dos prejuízos financeiros diretos, esses ataques podem levar ao roubo de dados sensíveis, comprometendo a segurança pessoal e corporativa. O impacto na reputação das empresas pode ser devastador, afetando a confiança dos clientes e parceiros. Um exemplo segundo discorre Veridian (2023) o ataque ao twitter (X) que resultou no comprometimento de várias contas verificadas de alto perfil, com o objetivo de realizar esquemas de fraude envolvendo criptomoedas, postando tweets enganosos que solicitavam doações em Bitcoin. Em casos extremos, esses ataques podem ameaçar a segurança nacional ao comprometer infraestruturas críticas.

Portanto, para combater eficazmente essas ameaças, é crucial adotar uma abordagem multifacetada que inclua tanto medidas comportamentais quanto tecnológicas. A conscientização desempenha um papel fundamental; portanto, é essencial promover o treinamento contínuo para funcionários, garantindo que todos estejam cientes das técnicas de engenharia social e saibam como reconhecer sinais de alerta.

Além disso, a verificação de informações deve ser uma prática padrão. Incentivar as pessoas a confirmar a autenticidade de e-mails, ligações e mensagens antes de responder ou clicar em links pode ajudar a prevenir muitos ataques. Promover uma cultura de desconfiança saudável também é vital, incentivando os indivíduos a questionar solicitações e informações não solicitadas. A combinação de conscientização, verificação cuidadosa e soluções tecnológicas robustas é a chave para minimizar os riscos e proteger tanto indivíduos quanto organizações contra a engenharia social. Com uma abordagem proativa e integrada, é possível reduzir significativamente o impacto desses ataques e fortalecer a resiliência das defesas de segurança.

3. IMPACTO NA PRIVACIDADE ONLINE

3.1. LEGISLAÇÃO E REGULAÇÃO

No Brasil, a legislação sobre proteção de dados e privacidade é regida principalmente pela Lei Geral de Proteção de Dados (LGPD), instituída pela Lei nº 13.709/2018. Esta legislação é uma resposta às preocupações crescentes com a privacidade online e estabelece normas rigorosas para a recolha, uso, armazenamento e partilha de dados pessoais. A LGPD tem como objetivo garantir que os dados pessoais sejam tratados de maneira transparente e responsável, oferecendo aos indivíduos maior controle sobre suas informações.

A LGPD determina que qualquer coleta de dados deve ser realizada com consentimento explícito do titular, exceto em situações específicas previstas na lei, como o cumprimento de obrigações legais ou a proteção da vida. As empresas e organizações são obrigadas a implementar medidas de segurança específicas para proteger os dados pessoais e notificar a Autoridade Nacional de Proteção de Dados (ANPD) e os titulares em caso de incidentes de segurança que possam comprometer a privacidade dos dados.

Além da LGPD, o Marco Civil da Internet (Lei nº 12.965/2014) estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Este marco legal define a neutralidade da rede, a privacidade dos usuários e a responsabilidade dos provedores de serviços de internet. O Marco Civil também exige que os provedores de serviços armazenem

registros de acesso por um período determinado e os disponibilizem às autoridades quando necessário, contribuindo para a segurança cibernética e a investigação de crimes virtuais.

A Lei Carolina Dieckmann (Lei nº 12.737/2012) também desempenha um papel relevante na proteção da privacidade online. Esta lei tipifica crimes relacionados à invasão de dispositivos eletrônicos e à divulgação não autorizada de dados, tendo sido criada em resposta ao caso de invasão de privacidade que envolveu a atriz Carolina Dieckmann. O artigo 154-A do Código Penal Brasileiro, introduzido por esta lei, define como crime a invasão de dispositivos eletrônicos, como computadores e smartphones, para acessar, obter ou divulgar dados sem autorização. A pena prevista é de reclusão de 6 meses a 2 anos, além de multa. A Lei Carolina Dieckmann é fundamental para a proteção de dados pessoais em um cenário onde a segurança digital é uma preocupação crescente.

Essas legislações, conjuntamente, fornecem um arcabouço regulatório robusto para a proteção da privacidade e segurança dos dados no ambiente digital, oferecendo mecanismos legais para combater a violação de dados e promover a segurança cibernética no Brasil.

3.2. PREVENÇÃO

Para mitigar os impactos negativos dos crimes cibernéticos na privacidade online, é crucial adotar uma abordagem proativa que combine medidas tecnológicas e comportamentais. A implementação de estratégias de prevenção pode ajudar a reduzir os riscos e proteger a integridade dos dados pessoais e corporativos. Medidas tecnológicas, como criptografia de dados[6], autenticação de dois fatores[7] e utilização de firewalls avançados[8], são essenciais para proteger sistemas e dados contra ataques cibernéticos. A segurança garante que as informações sejam codificadas e só possam ser acessadas por aqueles que possuem a chave adequada, enquanto a autenticação de dois fatores adiciona uma camada extra de segurança, exigindo que os usuários forneçam duas formas de identificação antes de acessar suas contas. (Barboza, *et al*,. 2024*)*

Além das soluções tecnológicas, a conscientização e a educação sobre segurança cibernética desempenham um papel fundamental na prevenção de fraudes e no combate ao roubo de dados. A formação contínua de funcionários e usuários sobre práticas seguras, como a verificação de e-mails e a identificação de sinais de phishing, é crucial para evitar que ataques

[6] É uma técnica que transforma informações em um código secreto, protegendo-as de acesso não autorizado.
[7] É um método de segurança que exige duas formas de identificação para acessar uma conta ou recurso.
[8] "*firewalls"* é um sistema de segurança de rede de computadores que restringe o tráfego da Internet para, de ou em uma rede privada.

de engenharia social e outros métodos fraudulentos comprometam a segurança. A promoção de uma cultura de segurança dentro das organizações, onde a proteção dos dados e a privacidade são priorizadas, também é vital. Incentivar os indivíduos a questionar a proteção de informações e adotar práticas seguras pode ajudar a prevenir muitos ataques e reduzir o impacto de incidentes de segurança.

Em resumo, a legislação brasileira, com a LGPD e o Marco Civil da Internet, estabelece um arcabouço regulatório robusto para a proteção de dados e privacidade online. A Lei Carolina Dieckmann também contribui para a proteção contra a invasão de dispositivos eletrônicos e a divulgação não autorizada de dados. No entanto, a eficácia dessas leis depende da implementação de medidas preventivas adequadas e da conscientização contínua sobre a segurança cibernética.

CONCLUSÃO

Este trabalho abordou os crimes cibernéticos e seu impacto na privacidade online, buscando compreender a evolução desses delitos e a eficácia da legislação brasileira no combate a essas ameaças. O objetivo principal foi analisar as lacunas existentes na legislação e propor soluções para aprimorar a proteção da privacidade dos indivíduos no ambiente digital.

A hipótese levantada, que afirmava que a legislação atual é insuficiente para lidar adequadamente com os crimes cibernéticos e garantir a privacidade online, foi confirmada. A discussão ao longo do trabalho revelou que, apesar da existência de leis como a Lei Geral de Proteção de Dados (LGPD) e a Lei Carolina Dieckmann, ainda há uma necessidade urgente de melhorias na implementação e fiscalização dessas normas, além de um maior investimento em educação e conscientização digital.

Além disso, é importante reconhecer o papel crescente da inteligência artificial e outras inovações tecnológicas que, apesar de facilitarem o avanço da segurança digital, também trazem novos desafios em termos de vulnerabilidades. A evolução dessas tecnologias demanda que as políticas públicas e as práticas de cibersegurança acompanhem essas mudanças de forma constante, com o intuito de garantir uma resposta eficaz às novas modalidades de crimes cibernéticos.

Outro aspecto que merece atenção é o desenvolvimento de estratégias preventivas que incluam a capacitação de profissionais especializados em segurança digital. A formação continuada e o desenvolvimento de ferramentas tecnológicas avançadas são essenciais para que o Brasil se mantenha alinhado com os padrões internacionais de combate aos crimes

cibernéticos. Somente com uma atuação conjunta entre o governo, o setor privado e a sociedade civil será possível enfrentar, de maneira eficaz, as ameaças impostas pela criminalidade virtual.

A análise desenvolvida mostrou que a crescente complexidade dos crimes cibernéticos exige uma abordagem multidisciplinar, envolvendo não apenas o âmbito jurídico, mas também a colaboração entre diferentes setores da sociedade. A falta de integração entre as legislações e a diversidade de abordagens adotadas por diferentes países dificultam a eficácia das medidas de proteção.

Em conclusão, a sociedade e o Estado devem trabalhar em conjunto para enfrentar os desafios impostos pelos crimes cibernéticos. O fortalecimento das leis, a promoção de campanhas educativas e a adoção de tecnologias de segurança mais eficazes são essenciais para assegurar a privacidade e segurança no ambiente digital. O sucesso no combate a esses crimes dependerá da adaptação das políticas públicas e do engajamento de todos os atores na defesa da privacidade online.

REFERÊNCIAS

ANDRION, Roseli. **História da segurança virtual:** A origem do cibercrime. 2021. Disponível em: https://canaltech.com.br/seguranca/historia-da-seguranca-virtual-a-origem-do-cibercrime-203073/. Acesso em: 04 out. 2023.

BARBOZA, Ana Clara Viveiros. *Et al.* Segurança Cibernética e o Direito. **Revista Humanidades** (**Montes Claros)**, Januária, v. 13, n. 1, 2024, ISSN 2526-656X.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [2016]. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 26 mai. 2024.

CANONGIA, Cláudia; JUNIOR, Raphael Mandariano. Segurança cibernética: o desafio da nova Sociedade da Informação. **Parcerias Estratégicas**, Brasília/DF, v. 14, n. 29, p. 21-46, jul-dez, 2009, ISSN 1413-9375.

CAMARA DOS DEPUTADOS. **Conheça a evolução dos crimes cibernéticos**. Disponível em: https://www.camara.leg.br/noticias/89137-conheca-a-evolucao-dos-crimes-ciberneticos. Acesso em: 10 jun. 2024.

CYBERCRIME. Portal da Interpol, s.d. Disponível em: https://www.interpol.int/en/Crimes/Cybercrime. Acesso em: 12 ago. 2024.

FIORILLO, Celso Antônio Pacheco; CONTE, Christiany Pegorari. **Crimes no meio ambiente digital e a sociedade da informação.** 2. ed. São Paulo: Saraiva, 2016.

POPPER, Marcos Antonio; BRIGNOLI, Juliano Tonizetti. **Engenharia Social:** um perigo iminente. Instituto Catarinense de Pós-Graduação, 2017.

OLIVEIRA, André Luis. *Et al.* **Multisaberes FADAT:** Direito e Educação: Pilares da Existência Social. 1. ed. Fortaleza: Mucuripe, 2024.

ROSA, Cinthia Danielle. *Et al.* Crimes Cibernéticos Contra Mulheres e o Ordenamento Jurídico. **Revista Brasileira de Estudos Jurídicos,** Montes Claros, v. 18, n.2, jul/dez. 2024, ISSN 1809-7278/2358-9744.

SANTOS, João Vitor Franco dos; ARAÚJO, Amanda de Campos. Cibersegurança e a Importância do Direito Digital. **Revista Multidisciplinar do Nordeste Mineiro**, v. 12, 2023. ISSN 2178-6925.

SERASA EXPERIAN**. Deepfake:** o que é, como identificar e proteger sua empresa. Disponível em: https://www.serasaexperian.com.br/conteudos/prevencao-a-fraude/deepfake/.Acesso em: 26 mai. 2024.

SILVEIRA, Marcelo; SANTOS, Clayton Eduardo dos. Crimes cibernéticos: um panorama geral sobre as principais ameaças. **Revista Científica e-Locução**, v. 1, n. 25, p. 25, 27 jun. 2024.

SIQUEIRA, Paulo Alexandre Rodrigues de. **O 'Deep Fake' e a Legislação Brasileira: utilização de instrumentos legais para a proteção à imagem.** 06 ago. 2019.

SOUZA, Ronaldo. **Prevenção de Fraudes Financeiras: Estratégias e Medidas de Proteção.** Disponível em: https://www.gov.br/investidor/pt-br/penso-logo-invisto/prevencao-de-fraudes-financeiras-estrategias-e-medidas-de-protecao. Acesso em: 17 set. 2024.

VERIDIAN, Maximiliano. **A face oculta da tecnologia: engenharia social e a arte da manipulação.** 2023. E-book Kindle.

WENDT, Emerson. JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos, Ameaças e Procedimentos de Investigação**. 3. ed. Rio de Janeiro: Brasport, 2021.