PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
PRO-REITORIA DE GRADUAÇÃO
ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO
COORDENAÇÃO DO CURSO DE DIREITO
NÚCLEO DE PRÁTICA JURÍDICA

MONOGRAFIA JURÍDICA

CRIMINALIDADE VIRTUAL

DESAFIOS DO DIREITO BRASILEIRO FACE O AVANÇO DOS CRIMES CIBERNÉTICOS

ORIENTANDO: PEDRO VINICIUS GUIMARÃES
ORIENTADOR: PROF. MS. ERNESTO MARTIM SCHÖNHOLZER DUNCK

GOIÂNIA-GO
2024

PEDRO VINICIUS GUIMARÃES

CRIMINALIDADE VIRTUAL

DESAFIOS DO DIREITO BRASILEIRO FACE O AVANÇO DOS CRIMES CIBERNÉTICOS

Monografia jurídica apresentado à disciplina Trabalho de Curso II, da Escola de Direito, Negócios e Comunicação do Curso de Direito da Pontifícia Universidade Católica de Goiás (PUC-GOIÁS).
Prof. Orientador: Ernesto Martim S. Dunck.

GOIÂNIA-GO
2024

PEDRO VINICIUS GUIMARÃES

CRIMINALIDADE VIRTUAL

DESAFIOS DO DIREITO BRASILEIRO FACE O AVANÇO DOS CRIMES CIBERNÉTICOS

Data da Defesa: 15 de maio de 2024

BANCA EXAMINADORA

_____ _____

Orientador: Prof. Ernesto Martim S. Dunck Nota

_____ _____

Examinador Convidado: Prof. Júlio Anderson Alves Bueno Nota

SUMÁRIO

AGRADECIMENTOS

Agradeço a Deus por ter me guiado ao longo desta jornada. Sou grato aos meus pais, tios e tias, que sempre me apoiaram e acreditaram em mim. Agradeço aos professores que me proporcionaram conhecimento e aos amigos que me acompanharam durante esta trajetória.

EPÍGRAFE

Na era digital, a fronteira entre liberdade e os crimes cibernéticos é tão fina quanto um *byte,* e tão crucial quanto a segurança de toda uma sociedade.

RESUMO

O presente trabalho busca entender o avanço da tecnologia que trouxe consigo um aumento significativo nos crimes cibernéticos, representando uma ameaça global. Este trabalho aborda essa problemática, investigando suas causas, impactos e estratégias de prevenção. A análise revela que a falta de conscientização sobre segurança digital, a rápida evolução tecnológica e a impunidade contribuem para a proliferação desses crimes. Os impactos são vastos, incluindo perdas financeiras, violações de privacidade e danos à reputação. Para enfrentar esse desafio, são necessárias abordagens multifacetadas, que combinem medidas técnicas, legais e educacionais. A implementação de sistemas de segurança robustos, leis atualizadas e campanhas de conscientização podem ajudar a mitigar os riscos. Além disso, a cooperação internacional e o compartilhamento de informações são essenciais para combater eficazmente os crimes cibernéticos. Este estudo destaca a urgência de ações coordenadas e proativas para proteger a sociedade digital contra essa ameaça em constante evolução.

Palavras-chave: Cibercrime, Internet, Impactos, Prevenção.

ABSTRACT

This work seeks to understand the advancement of technology that has brought with it a significant increase in cybercrimes, representing a global threat. This work addresses this problem, investigating its causes, impacts and prevention strategies. The analysis reveals that the lack of awareness about digital security, rapid technological evolution and impunity contribute to the proliferation of these crimes. The impacts are vast, including financial losses, privacy breaches and reputational damage. To address this challenge, multifaceted approaches are needed, combining technical, legal and educational measures. Implementing robust security systems, updated laws and awareness campaigns can help mitigate risks. Furthermore, international cooperation and information sharing are essential to effectively combat cybercrime. This study highlights the urgency of coordinated and proactive actions to protect digital society against this constantly evolving threat.

Keywords: Cybercrime, Internet, Impacts, Prevention.

INTRODUÇÃO

O presente trabalho tem como objeto o estudo dos crimes cibernéticos, entender os desafios da legislação brasileira e da sociedade no enfrentamento aos cibercrimes. Com a evolução da tecnologia, os cibercrimes se tornaram uma ameaça real, com exemplos que vão desde os primeiros hackers até os ataques cibernéticos em larga escala da atualidade, como *ransomware* e *phishing*. Esse desenvolvimento histórico é essencial para compreender a complexidade e a crescente importância dos cibercrimes na sociedade contemporânea, além dos tipos de crimes cibernéticos, e como eles abrangem uma ampla gama de atividade ilícitas que exploram as vulnerabilidades do ambiente digital.

Os crimes cibernéticos, conceituados como atividades ilegais perpetradas no ambiente virtual, abrangem uma ampla gama de comportamentos criminosos que exploram a tecnologia para diversos fins ilícitos. Esses crimes são categorizados de acordo com a utilização de ferramentas eletrônicas, desde a criação de *softwares* maliciosos até a prática de fraudes online e violações de dados. A diversidade e a constante evolução desses delitos exigem uma compreensão abrangente dos conceitos e tipos de crimes cibernéticos, a fim de implementar medidas de segurança eficazes.

Nesse contexto, o presente trabalho também busca entender a vulnerabilidade da *internet*, apontando como a complexidade tecnológica e a falta de padrões universais de segurança como desafios no combate aos crimes cibernéticos. A compreensão do contexto histórico, dos conceitos e tipos de crimes cibernéticos, bem como das vulnerabilidades da internet, destaca a necessidade de uma abordagem abrangente e colaborativa para combater eficazmente a cibercriminalidade.

Neste trabalho, serão abordados os impactos dos cibercrimes em diferentes esferas da sociedade, destacando aspectos econômicos, de privacidade, segurança nacional, crime organizado, psicológicos, inovação tecnológica e legais. Economicamente, os cibercrimes representam custos significativos para empresas e governos, incluindo perdas financeiras diretas e custos de recuperação de dados. Além disso, comprometem a privacidade ao expor dados pessoais e confidenciais, o

que mina a confiança nas instituições e causa impactos sociais significativos.

Os ataques cibernéticos também representam uma ameaça à segurança nacional, pois podem visar infraestruturas críticas e serem realizados por atores estatais ou organizações criminosas transnacionais. O crime organizado aproveita-se da cibercriminalidade para expandir suas atividades globalmente, enquanto as vítimas sofrem consequências emocionais sérias, como estresse, ansiedade e até traumas duradouros.

Além disso, a inovação tecnológica é prejudicada pela desconfiança na segurança cibernética, pelos custos adicionais para proteção, pela ameaça à propriedade intelectual e pelas dificuldades em cumprir regulamentações. Isso tudo mostra como os ataques cibernéticos têm um impacto profundo e amplo na sociedade atual.

Por outro lado, combater o cibercrime é uma tarefa complexa que requer uma abordagem diversificada, combinando políticas e tecnologias para lidar com ameaças em constante mutação. É crucial estabelecer leis e regulamentos específicos para tornar ilegais as atividades cibernéticas maliciosas e fornecer orientações claras para a aplicação da lei. Além disso, parcerias internacionais são fundamentais para identificar e responsabilizar os culpados, enquanto a colaboração entre os setores público e privado é essencial para compartilhar informações e desenvolver melhores práticas de segurança.

Assim, por meio da análise desses elementos, este trabalho visa fornecer *insights* valiosos sobre os desafios enfrentados na prevenção e combate aos crimes cibernéticos, destacando a necessidade de cooperação internacional, inovação tecnológica e reformas legislativas para proteger efetivamente o ambiente virtual e preservar a integridade das sociedades digitais.

O presente trabalho foi elaborado com base em livros, artigos científicos, documentos e estudos de caso. Tem caráter teórico, explicativo e descritivo, incluindo uma investigação, registro, análise e interpretação de fenômenos atuais, visando compreender o seu funcionamento no contexto presente. O objetivo é aprofundar o conhecimento sobre o tema abordado, destacando os pontos mais relevantes e criteriosos.

O primeiro capítulo discutirá aspectos históricos e conceituais relacionados à internet e à cibercriminalidade, explorando sua origem e evolução, bem como analisando a identidade dos cibercriminosos.

O segundo capítulo abordará os impactos dos cibercrimes no contexto geral da sociedade.

O terceiro capítulo explora sobre as estratégias para o combate aos cibercrimes, desde suas primeiras medidas até a legislação vigente.

I. CRIMES CIBERNÉTICOS

1.1. CONTEXTO HISTÓRICO

Primeiramente, para compreender o tema, se faz necessário entender o contexto em que o presente tema surgiu. Os crimes cibernéticos, tem uma história intrincada que remonta às origens da tecnologia da *internet* e da informação. No final da década de 40, os primeiros computadores foram desenvolvidos, principalmente para fins acadêmicos e governamentais. Desde esse período, diversos incidentes que poderiam ser considerados como “crimes cibernéticos” começaram a aparecer, contudo, como a conectividade era limitada, e a noção dos *cibercrimes* como conhecemos hoje em dia estava longe de se concretizar.

Porém, no final da década de 60, virada para a década de 70 surgiu a *ARPANET* (Advanced Research Projects Agency Network), que foi a precursora da *internet* moderna, cujo principal intuito era para fins de pesquisa e comunicação militar entre os departamentos de pesquisas dos Estados Unidos. O termo “*internet*” surgiu décadas após, quando a *internet* passou a ser utilizada por universidades americanas. Conforme a *internet* se expandia, expandia também a oportunidade para atividades criminosas.

Na década de 1980 surgiu uma comunidade de *hackers* e a disseminação de vírus de computador, tais eventos marcaram a consolidação dos crimes cibernéticos com uma ameaça real e presente.

Com a popularização da *internet* na década de 1990 trouxe uma explosão de atividade criminosa no ambiente virtual, golpes, fraudes financeiras e crimes envolvendo cartões de crédito foram se tornando comuns. Iniciava-se o desenvolvimento de regulamentações e leis voltadas para os *cibercrimes*. Já nos anos 2000 iniciou os ataques *cibernéticos* em larga escala.

Atualmente os crimes cibernéticos evoluíram significativamente. *Ransomware,* ataques de *phishing superelaborados*, vazamentos de dados em grande escala e invasões de sistemas corporativos são bem comuns. A sofisticação de tais crimes demanda uma resposta equiparada por parte da segurança cibernética e da legislação.

É perceptível que a *internet*, interpreta um importante papel na sociedade, prestando serviços para o governo, segurança, economia, educação…

espalhando-se por todo e qualquer tipo de relação, seja comercial, social, cultural e pessoal. Devido à crescente dependência da sociedade em relação à tecnologia da informação, o cibercrime emergiu como um fenômeno internacionalmente crescente e recorrente. Isso tem resultado na violação dos direitos fundamentais das pessoas, à medida que criminosos aproveitam as vulnerabilidades do ambiente digital.

De acordo com Simas (2014, p 14).

> A evolução operada nas novas tecnologias, projectou-se sobre o fenômeno criminal, pois se atendermos às suas duas vertentes, por um lado, a tecnologia poder, ela mesma, objecto de prática de crimes e por outro lado, suscita e potência novas formas criminais ou novas formas de práticas antigos crimes.

Assim, o contexto histórico dos *cibercrimes* demonstra uma evolução contínua, desde os primórdios da computação até os desafios atuais da era digital, compreender tal história é fundamental para lidar de forma eficaz com os crimes cibernéticos, desenvolvendo assim, estratégias de segurança e leis adequadas a um ambiente virtual em constante evolução.

1.2. CONCEITOS E TIPOS

É sabido que os crimes cibernéticos consistem no cometimento de atividades ilícitas praticadas no ambiente virtual, que abrangem uma vasta variedade de atividades criminosas que envolvem o uso da internet, dispositivos eletrônicos como meios para cometer delitos.

Nesse sentido, é válido citar Rosa (2002, p. 53) que conceitua os crimes da internet como:

> A conduta atenta contra o estado natural dos dados e recursos oferecidos por um sistema de processamento de dados, seja pela compilação, armazenamento ou transmissão de dados, na sua forma, compreendida pelos elementos que compõem um sistema de tratamento, transmissão ou armazenagem de dados, ou seja, ainda, na forma mais rudimentar; 2. O „Crime de Informática‟ é todo aquele procedimento que atenta contra os dados, que faz na forma em que estejam armazenados, compilados, transmissíveis ou em transmissão; 3. Assim, o “Crime de Informática‟ pressupõe dois elementos indissolúveis: contra os dados que estejam preparados às operações do computador e, também, através do computador, utilizando-se software e hardware, para perpetrá-los; 4. A expressão crimes de informática, entendida como tal, é toda a ação típica, antijurídica e culpável, contra ou pela utilização de processamento automático e/ou eletrônico de dados ou sua transmissão; 5. Nos crimes de informática, a ação típica se realiza contra ou pela utilização de processamento automático de dados ou a sua transmissão. Ou seja, a utilização de um sistema de informática para atentar contra um bem ou interesse juridicamente protegido, pertence à ordem econômica, à

> integridade corporal, à liberdade individual, à privacidade, à honra, ao patrimônio público ou privado, à Administração Pública, etc.

No mesmo sentido, a Organização das Nações Unidas (ONU) adotada o seguinte conceito em relação aos crimes cibernéticos o seguinte:

> Os crimes cibernéticos são uma forma de crime transnacional em expansão. Sua natureza complexa de crime que ocorre no ciberespaço, sem fronteiras, é agravada pelo crescente envolvimento de grupos do crime organizado.

Desse modo, observa-se que os crimes cometidos no ambiente virtual são conceituados no geral como qualquer atividade criminosa que envolvam o uso da tecnologia no ambiente digital.

Existem diversas classificações doutrinárias que definem os *cibercrimes*. Damásio de Jesus, por exemplo, faz a divisão dos crimes virtuais em duas classes: próprios, impróprios. Segundo ele, os crimes virtuais próprios são aqueles em que o perpetrador necessariamente utiliza ferramentas eletrônicas para cometer o delito. Ou seja, esses crimes não podem ser cometidos sem o uso de um computador, já que o computador é um elemento intrínseco à prática do crime. Alguns exemplos de crimes virtuais próprios incluem ataques de vírus e *malware*. Damásio ainda acrescenta que nesses crimes virtuais próprios, a informática, incluindo a segurança dos sistemas, a titularidade das informações e a integridade dos dados e dos dispositivos, é o objeto jurídico protegido.

Ademais, é o que estabelece o Art. 5º, inciso LXXIX da Constituição Federal de 1988:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes
> (...)
> LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.
> (...)

Segundo Damásio (Manual dos crimes informáticos, 2016), os crimes virtuais impróprios são aqueles em que o computador é utilizado como uma ferramenta para a execução de condutas que já são consideradas ilícitas de acordo com a legislação existente. Em outras palavras, a internet é usada como uma nova forma de cometer “velhos crimes”, como pedofilia e tráfico de órgãos, que já eram proibidos mesmo antes da era digital. Nesses casos, a tecnologia da informação é empregada como meio para a perpetração de crimes que já eram considerados

ilegais.

Ainda, a Convenção de Budapeste adota como conceito para os crimes *cibernéticos* o seguinte (UNDOC, 2023):

> comportamentos ilícitos que violem normas sociais e leis nacionais, perpetrados através da utilização de sistemas de informação e redes de computadores, com o intuito de causar danos a indivíduos, organizações ou estados, comprometendo a integridade, confidencialidade e disponibilidade de dados e sistemas.

Diante o exposto, nota-se que os conceitos de crimes *cibernéticos* abrangem uma ampla gama de atividades ilícitas que exploram a vulnerabilidade no ambiente digital. Mas no geral todos referem-se a atividades delituosas perpetradas no meio digital.

Assim, conceituado os crimes cibernéticos, pode-se tratar dos principais tipos de cibercrimes cometidos no ambiente virtual, sendo eles:

a) Pirataria: que é a cópia e distribuição não autorizada ou uso indevido de *software*, música, filmes, livros, jogos ou outros conteúdos protegidos por direitos autorais.

b) *Phishing:* Uma prática em que os crimes tentam obter informações confidenciais, senhas e detalhes financeiros, enganando as pessoas para que forneçam tais informações, muitas das vezes por meio de e-mails ou sms falsos.

c) *Malware*: Que são *softwares* maliciosos projetados para danificar, controlar ou roubar informações de um sistema.

d) *Hacking:* Acesso não autorizado por meio de vulnerabilidades de sistemas de computadores ou redes para explorar, modificar e roubar informações.

e) Roubo de Identidade: Está tipificado no Art. 307 do Código Penal “Atribuir-se ou atribuir a terceiro falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem”, ou seja, é o uso não autorizado de informações pessoais para cometer fraudes, geralmente com o objetivo de obter benefícios financeiros.

f) Fraude Online: Atividades fraudulentas, como esquemas de pirâmide, falsificação de identidade, ou venda de produtos inexistentes.

g) *Ciberespionagem*: Roubo de informações sensíveis, muitas vezes realizadas por governos ou grupos organizados, com o intuito de obter vantagens políticas, econômicas ou militares.

h) Violação de dados: Acesso não autorizado e divulgação de informações pessoais ou empresariais.

i) Assédio Online: Comportamentos hostis, como *cyberbullying, stalking* ou disseminação de discurso de ódio na internet.

j) Fraude Financeira: Manipulação de transações financeiras online para benefício próprio, como roubo de cartões de crédito ou falsificação de transações.

Esses exemplos são apenas alguns, dos diversos cibercrimes e a lista continua a se expandir conforme as tecnologias avançam e novas oportunidades para cibercriminalidade surgem. Assim, levando em consideração que os *cibercrimes* é um campo amplo e em constante evolução devido aos inevitáveis avanços tecnológicos, para combater de forma eficaz esses delitos, é de suma importância que os governos, empresas e indivíduos no geral estejam cientes dos diversos conceitos e tipos de *cibercrimes*, para que adotem medidas de segurança mais adequadas.

Em resumo, o conceito de crimes *cibernéticos* representa uma preocupação crescente em uma era profundamente impulsionada pela tecnologia da informação. A constante evolução das ferramentas digitais trouxeram consigo significativos desafios, que resultaram em uma vasta gama de atividades ilícitas que favorecem a vulnerabilidade da *internet*. Assim, a colaboração internacional torna-se crucial na mitigação dessas ameaças transnacionais, evidenciando a necessidade de contínuos avanços na segurança cibernética, legislação e aplicação da lei para preservar a integridade do *ciberespaço* e garantir a proteção contra potenciais danos causados por criminosos nos meios digitais.

1.3. VULNERABILIDADE DA *INTERNET*

Desde o princípio o mundo funciona como uma engrenagem, que é uma peça fundamental para o desenvolvimento da sociedade e para harmonia entre as comunidades, quando falamos em harmonia é natural lembramos das Leis e do Direito, pois são estes que facilitam o relacionamento entre a população, sendo essenciais para o progresso social.

Nos dias atuais pode-se observar uma instabilidade acompanhada de

fanatismos, esse cenário gera desequilíbrios políticos, sociais e econômicos. Estamos imersos em um século no qual a tecnologia está promovendo inúmeras transformações. No entanto, é crucial destacar a importância de uma abordagem equilibrada ao adentrar o mundo digital, uma vez que a exploração desenfreada pode resultar em riscos para o usuário, dadas as diversas camadas digitais que podem se tornar perigosas durante o acesso indiscriminado. O uso responsável e consciente da tecnologia é vital para mitigar potenciais impactos negativos nas esferas política, social e econômica.

Nesse sentido, com as diversas facilidades e possibilidades que a *Internet* proporciona pode-se citar (Lisboa, 2016, p. 10):

> Essas facilidades estão tão em evidência no cotidiano que não há uma percepção clara de que se vive em uma sociedade informatizada, onde os dados fluem a velocidades inimagináveis há alguns anos, e tudo isso influi em nos valores sociais e econômicos.

A vulnerabilidade da internet pode ser relacionada a diversos fatores, como a complexidade tecnológica, uma vez que a *internet* é composta de sistemas complexos, servidores e dispositivos, o que consequentemente cria diversas oportunidades de vulnerabilidade. O desenvolvimento rápido e constante de novas tecnologias muitas das vezes supera a capacidade de se implementar novas medidas de segurança mais eficazes.

A vulnerabilidade da *internet* é uma realidade natural à sua complexidade e interconectividade global. A rápida evolução tecnológica, aliada à falta de padrões universais de segurança, cria um terreno fértil para ameaças *cibernéticas*. A dependência generalizada da *internet* para uma variedade de atividades, desde comunicação até transações financeiras, amplia as possibilidades de ataques cibernéticos.

Falhas em *software* e *hardware*, aliadas a ataques cibernéticos cada vez mais sofisticados, destacam a necessidade urgente de abordar vulnerabilidades para proteger dados sensíveis e preservar a integridade da infraestrutura digital. A questão da privacidade e os desafios jurídicos em uma rede global acrescentam camadas adicionais de complexidade, exigindo esforços coordenados e inovação contínua para fortalecer a segurança da *internet* e mitigar riscos inerentes.

Apesar de já existirem leis específicas que tratam do tema, estão longe de serem 100% eficazes contra a evolução dos cibercrimes. A velocidade com que as

novas formas de ataques surgem supera a capacidade dos sistemas jurídicos e das legislações responderem de forma eficiente.

Com a falta de uniformidade nas legislações entre os países, cria precedentes legais que são explorados pelos criminosos no ambiente virtual, desafiando as capacidades das autoridades de aplicarem a lei de maneira consistente e eficaz, essa lacuna entre a evolução dos crimes cibernéticos e a lentidão na adaptação das estruturas legais destaca a urgência de reformas legislativas que estejam a frente da evolução dos cibercrimes, para enfrentar adequadamente os desafios crescentes dos crimes cibernéticos.

Em uma última análise, observa-se que a vulnerabilidade da *internet* é um lembrete contundente de que, embora essa rede global tenha revolucionado e continua revolucionando a forma como vivemos, trabalhamos, estudamos e nos conectamos, ela não está imune aos crimes, a interconexão massiva de dispositivos e sistemas, aliada à rápida evolução tecnológica, expõe a *internet* a diversas vulnerabilidades e ameaças cibernéticas.

Para que as medidas contra a cibercriminalidade tenham maior eficácia de nada adianta apenas avanços em protocolos de segurança, mas também uma mudança fundamental na mentalidade da população, promovendo uma cultura de cibersegurança e colaboração global. Somente por meio de esforços coordenados e inovadores podemos fortalecer a vulnerabilidade da internet e amortecer os impactos potencialmente devastadores de sua vulnerabilidade.

II. IMPACTOS DOS CIBERCRIMES

2.1. IMPACTOS DOS CIBERCRIMES EM DIFERENTES ASPECTOS

A cibercriminalidade tem uma série de impactos em diferentes aspectos da sociedade, da economia e segurança.

2.2. IMPACTO ECONÔMICO

O impacto econômico é um dos principais impactos decorrentes do cibercrime, eles têm um custo significativo para empresas e governos ao redor do mundo, podem resultar em uma perda de receita devido ao roubo de propriedade

intelectual, interrupções de serviços, fraudes financeiras e custos de recuperação de dados, para recuperar dados, reparar sistemas comprometidos e mitigar os danos causados pelos cibercrimes.

Além disso, os cibercrimes diariamente resultam em perdas financeiras diretas, como fraudes bancárias, roubo de informações confidenciais e extorsões, essas atividades criminosas não apenas causam danos imediatos às organizações, mas também tem o potencial de minar a confiança dos clientes e investidores, afetando negativamente a reputação e credibilidade das empresas, podendo acarretar em perdas adicionais de receita e novas oportunidades de negócios.

Segundo pesquisa da statista.com, o custo estimado dos crimes cibernéticos, no mercado de segurança cibernética aumentasse continuamente entre 2023 e 2028 em um total de 5,7 trilhões de dólares, após o décimo primeiro ano consecutivo de aumento, estima-se que o indicador atinja 13,82 biliões de dólares até 2028.

Ademais, o aumento dos custos de segurança cibernética e as perdas econômicas resultantes dos cibercrimes representam um desafio significativo para o desenvolvimento econômico sustentável e para a inovação tecnológica, afetando o bem-estar econômico global.

2.3. IMPACTO NA PRIVACIDADE

Os cibercriminosos frequentemente buscam informações pessoais e confidenciais, o que acarreta nos impactos da privacidade, antes considerada um direito fundamental na era digital, agora está constantemente sob ameaça das atividades cibercriminosas, uma das principais maneiras pelas quais os cibercriminosos impactam na privacidade é por meio da violação de dados. Grandes corporações, instituições governamentais a até mesmo pequenas empresas são alvos frequentes dos ataques cibernéticos, o que resulta nos vazamentos massivos de informações de milhões de pessoas, tais violações não apenas expõem informações sensíveis, mas também diminuem a confiança do público nas instituições que deveriam assegurar seus dados.

Ademais das violações de dados, os cibercrimes envolvem práticas como o *phishing*, na qual os criminosos enganam as pessoas para revelarem informações pessoais, e o *spyware*, que permite o monitoramento das atividades online de um

indivíduo sem seu conhecimento ou consentimento, essas práticas comprometem a privacidade individual, mas também podem levar a consequências graves, como roubo de identidade e extorsão.

Outro aspecto importante para ser considerado em relação a prevenção da privacidade é a questão da vigilância em massa, governos e agências de inteligências em todo o mundo têm utilizado técnicas de monitoramento em larga escala, muitas das vezes sem consentimento dos cidadãos, o que levanta preocupações significativas sobre a privacidade e liberdade civis, criando um ambiente onde a vida privada é constantemente invadida em nome da segurança pública e nacional.

Além dos impactos individuais, as violações de privacidade têm consequências mais abrangentes para a sociedade, a perda de confiança nas instituições e na segurança dos dados pode prejudicar a adoção de novas tecnologias e inovações, atrasando o progresso e o desenvolvimentos em diversas áreas da sociedade. Assim, os cibercrimes representam uma ameaça significativa à privacidade e segurança das informações na era digital.

2.4. IMPACTO NA SEGURANÇA NACIONAL

Os impactos dos crimes cibernéticos na segurança nacional são cada vez mais aparentes e preocupantes, pois as ameaças cibernéticas podem ter consequências avassaladoras para os governos e para as populações.

Os ataques contra a infraestruturas críticas, como sistemas de energia, transporte, comunicação e serviços financeiros, representam uma ameaça direta à segurança nacional de um país, interrupções nessas áreas essenciais podem causar o caos social, desestabilizando a economia a até mesmo colocar vidas em risco, diminuindo a capacidade do Estado de garantir a segurança de seus cidadãos.

Para além disso, os cibercrimes muitas das vezes são perpetrados por atores estatais hostis, terroristas ou até mesmo organizações criminosas transnacionais, que visam não somente causar danos financeiros, mas também comprometer a soberania nacional e a segurança de um país. Os ataques cibernéticos podem ser utilizados como um meio de espionagem industrial, para a obtenção de segredos militares, sabotagem de operações militares e desestabilização política, o que representa uma ameaça significativa para a

segurança nacional e para a integridade dos sistemas governamentais.

A natureza transnacional dos cibercrimes apresenta um desafio adicional para a segurança nacional, uma vez que os atores cibernéticos podem operar além das fronteiras nacionais terrestres, aproveitando lacunas na cooperação internacional e na aplicação da lei para fugirem da responsabilidade e escapar das sanções e consequências de suas ações. Isso torna difícil para os governos protegerem suas infraestruturas críticas, combaterem ameaças cibernéticas e garantirem a segurança virtual de duas nações em um ambiente global cada vez mais interconectado e interdependente.

Em síntese, os impactos dos crimes cibernéticos na segurança nacional são profundos e complexos, exigindo uma abordagem coordenada e abrangente por parte dos governos e da comunidade internacional para enfrentar as crescentes ameaças à estabilidade e à segurança global.

2.5. IMPACTO NO CRIME ORGANIZADO

Por várias vezes, os cibercriminosos são perpetrados por grupos criminosos organizados que operam globalmente, tais grupos podem se envolver em uma variedade de atividades criminosas, como as fraudes financeiras, extorsão, tráfico de drogas e humano, utilizando da *internet* para facilitar e expandir suas operações criminosas. O crime organizado na cibercriminalidade oferece uma maneira relativamente segura e lucrativa de cometer uma ampla gama de crimes, muitas das vezes sem deixar qualquer tipo de rastro ou vestígio para uma possível identificação dos criminosos.

Para o crime organizado uma das principais vantagens para em relação aos crimes cibernético é a possibilidade de operar em uma escala global, que contorna fronteiras físicas e desafia as autoridades policiais de diferentes países, além de proporcionar uma fonte de receita significativa para o crime organizado, permitindo que esses grupos lucre com uma ampla variedade de atividades criminosas sem os riscos associados ao tráfico de drogas ou outro meio ilícito tradicional de conseguir receita.

2.6. IMPACTO PSICOLÓGICO

Os cibercrimes podem ter uma série de impactos psicológicos nas vítimas, que podem variar de gravidade a depender da natureza do crime e das circunstâncias individuais. Uma das principais consequências é o estresse emocional e a ansiedade resultantes da violação da privacidade e da sensação de vulnerabilidade, a perda de controle sobre as informações pessoais e a exposição às ameaças online contribuem para que as vítimas tenham o sentimento de medo e insegurança, afetando sua saúde mental e bem-estar.

Para além disso, o impacto dos cibercrimes pode se estender além da vítima imediata, afetando também as relações interpessoais e sociais da vítima. Por exemplo, vítimas do roubo de identidade podem enfrentar a desconfiança e dificuldade de relacionamento com os amigos, familiares e colegas, pelo fato de tentarem lidar com as consequências do crime. O descrédito associado a ser uma vítima dos crimes cibernéticos também pode levar a vítima a sentimentos de vergonha e isolamento, impedindo as pessoas de buscar assistência.

Segundo pesquisa da *Security Leaders,* revela que mais de 40% dos crimes cibernéticos envolvem manipulação psicológica, segundo o mapeamento das violações mais recorrentes, aponta que próximo dos 40% das ocorrências envolveram engenharia social, 25% foram ataques via web, e 20% com invasão de sistemas. Entre as ações mais comuns, 85% das violações envolvem um elemento humano e 61% dos casos tiveram como finalidade o roubo de credenciais, e a maior parte dos ataques, 80%, parte de instituições criminosas altamente organizadas, que tem o intuito de lucrar de alguma forma com esses crimes.

A pesquisa ainda aponta que as principais mudanças nos tipos de violações ocasionadas pela pandemia do COVID-19, foram os casos de *phishing*, que nada mais é do que a técnica de enganar usuários e obter informações confidenciais, como os nomes de usuário e senhas. Outra ameaça que também cresceu na pandemia foram os ataques de *ransomware*, que são *malwares* que sequestram os dados da vítima, permitindo que os cibercriminosos peçam um “resgate” pela devolução e não divulgação dos dados.

Além disso, as vítimas dos crimes cibernéticos também podem experimentar traumas emocionais duradouros, principalmente se o crime envolver ameaças físicas ou sexuais, mesmo não existindo contato direto com o agressor, a natureza intrusiva e invasiva dos cibercrimes podem deixar uma marca psicológica profunda nas vítimas, causando sintomas de estresse pós-traumático e dificuldade

de recuperação. Em suma, os crimes cibernéticos podem ter uma vasta gama de impactos psicológicos nas vítimas, que vão desde o estresse, ansiedade até problemas mais graves de saúde mental.

2.7. IMPACTO NA INOVAÇÃO TECNOLÓGICA

Os crimes cibernéticos podem ter impactos significativos nas inovações tecnológicas de diferentes formas.

a) A Desconfiança na segurança cibernética: sem dúvidas é um dos principais impactos da cibercriminalidade, uma vez que criam um clima de desconfiança em relação à segurança cibernética, desencorajando empresas e usuários finais de aderirem novas tecnologias, a falta de confiança nas seguraça de dados pode retardar a implementação de novas tecnologias, principalmente naquelas que dependem de armazenamento e processamento de dados online.

b) Custos adicionais de segurança: várias empresas por diversas vezes precisam aumentar seus gastos com segurança cibernéticas, com o intuito de proteger suas redes e sistemas operacionais contra ameaças virtuais, o que pode representar ônus financeiros significativos, especialmente para startups e empresas de menor porte que podem ter recursos limitados para investir na segurança virtual. O direcionamento de recursos adicionais para segurança cibernética o que pode reduzir os investimentos em pesquisa e desenvolvimento de novas tecnologias.

c) Ameaças à propriedade intelectual: cibercriminosos frequentemente visam a propriedade intelectual valiosa, como algoritmos, designs e segredos comerciais. O roubo ou desvio desses ativos podem desencorajar as empresas de investir em pesquisas e desenvolvimento de novas tecnologias, tremendo que suas inovações sejam roubadas ou replicadas por seus concorrentes.

d) Dificuldade de conformidade regulatória: com a crescente complexidade das leis e regulamentos relacionados à segurança cibernética pode representar um desafio para as empresas que visam desenvolver e implementar tecnologias novas. O cumprimento das regulamentações de segurança virtual pode exigir recursos adicionais e atrasar o processo de inovações, principalmente para

empresas em setores altamente regulamentados, como saúde e financeiro.

e) Danos à reputação: os incidentes relacionados à segurança cibernética, com violações de dados.

2.8. IMPACTO LEGAL

Os crimes cibernéticos têm impactos legais significativos principalmente no que diz respeito ao contexto brasileiro, exigindo respostas abrangentes e adaptativas das autoridades e do sistema legal do país. No Brasil, as leis relacionadas à cibercriminalidade estão em constante evolução tentando acompanhar o rápido desenvolvimento das tecnologias digitais e as novas formas de atividades criminosas no ambiente virtual.

A principal área afetada é a legislação penal, o Brasil possui algumas legislações específicas para os crimes cibernéticos, como a lei nº 12.737/2012, conhecida como lei Carolina Dieckmann, que foi a primeira a tratar penalmente sobre os crimes cibernéticos, onde tipifica delitos como invasão de dispositivos informáticos e obtenção não autorizada de dados.

De igual modo, com a entrada em vigor da Lei nº 12.737/2012, o Código Penal Brasileiro passou a tipificar o crime de invasão de Dispositivo informático:

> Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita:
>
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa

Para além disso, os cibercrimes também tem implicações legais nas áreas como como o direito do consumidor, privacidade e proteção de dados, no Brasil existe também a Lei nº 13.709/2018, conhecida como a Lei Geral de Proteção de Dados (LGPD), que foi inspirada no Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, que estabelece diretrizes para o tratamento dos dados pessoais e impõe penalidades para violações de segurança cibernética e vazamento de dados.

A Lei Geral de Proteção de Dados (LGPD) tem como meta resguardar os direitos de liberdade, privacidade e o desenvolvimento livre da pessoa, promovendo segurança jurídica por meio de regulamentação e práticas que assegurem a proteção dos dados pessoais de todas as pessoas que estejam no território

brasileiro.

Contudo, o maior desafio reside na aplicação eficaz dessas leis, especialmente diante da transnacionalidade dos crimes cibernéticos e da dificuldade em identificar, localizar e punir os culpados, nesse sentido, vale ressaltar a natureza global da *internet*, muitos cibercriminosos operam além das fronteiras nacionais, tornando a cooperação entre países algo essencial para investigar, processar e punir os responsáveis pelos cibercrimes.

O Brasil participa de acordos e tratados internacionais para fortalecer a cooperação e a troca de informações entre as autoridades policiais e judiciárias de diversos países, mas nem sempre os acordos e tratados garantem que os cibercriminosos sejam localizados e punidos.

III. ESTRATÉGIAS POLÍTICAS E TECNOLÓGICAS EM RESPOSTA AO CIBERCRIME

As respostas ao cibercrime devem adotar uma abordagem abrangente que combine estratégias políticas e tecnológicas, com isso pode-se dizer que a implementação de leis e regulamentos eficazes são fundamentais para enfrentar o cibercrime. A criação de legislações específicas que criminalizem o cibercrime e forneçam diretrizes claras para a aplicação da lei são essenciais, nesse sentido já existem leis que tratam do tema, como a Lei nº 12.737/12, e ainda existem muitas em discussão.

Segundo Silva, as leis tiveram que se atualizar com o avanço tecnológico (Silva, 2003, p 28):

> O aparecimento da Informática no meio social ocorreu de forma tão rápida e passou a exigir, com a mesma rapidez, soluções que o Direito não estava preparado para resolver. Com isso, a necessidade social aparenta estar desprovida da tutela do Direito e a busca ansiosa por regular a matéria pode provocar a criação de leis excessivas e desnecessárias.

É crucial a implementação de políticas robustas de combate ao cibercrime, isso envolve o desenvolvimento e a aplicação de leis e regulamentos que criminalizem as atividades cibernéticas maliciosas, todavia, a utilização inadequada das técnicas e procedimentos informáticos, podem gerar impactos relevantes nas relações jurídicas, se utilizadas de qualquer maneira.

Estabelecer parcerias e acordos de colaboração entre países é

fundamental para garantir que os responsáveis pelos crimes cibernéticos sejam identificados e responsabilizados. Além disso, é fundamental incentivar a colaboração entre os setores público e privado para compartilhar informações sobre ameaças cibernéticas e desenvolver melhores práticas de segurança.

Em se tratando das estratégias tecnológicas, essas desempenham um papel crucial na prevenção e na mitigação do cibercrime, investir em pesquisa e desenvolvimento de tecnologias de segurança avançadas, como inteligência artificial, pode fortalecer as defesas virtuais e ajudar a identificar e neutralizar possíveis ameaças de forma mais eficaz e contundente. Ademais, a implementação de medidas de criptografia robustas e a melhoria da segurança de infraestrutura críticas são passos fundamentais para a proteção contra os ataques cibernéticos que possam causar danos significativos.

Para além das estratégias políticas e tecnológicas, a educação e a conscientização são fundamentais na luta contra os cibercrimes, educar a população sobre os possíveis riscos do cibercrime e ainda, promover boas práticas de segurança cibernética são essenciais. Além dessas estratégias, é essencial monitorar e analisar continuamente as ameaças à segurança cibernética, criar capacidades de resposta a incidentes e reforçar a infraestrutura para evitar ataques.

A colaboração internacional é fundamental na luta contra o crime cibernético, sendo essencial uma abordagem coordenada e colaborativa entre os países para combater as ameaças em nível global, uma vez que os crimes virtuais são difíceis de serem identificados.

Nesse sentido, pode-se citar o seguinte (Rosa, T, 2007, p. 5):

> (...) Podemos constatar, portanto, que é imprescindível que o legislador penal elabore normas próprias para coibir tais práticas delitivas, no caso, os chamados “crimes de informática”. Para isso, é necessário, entretanto, identificá- los, diferenciá-los e conceituá-los, propiciando assim leis mais claras e específicas, de forma a alcançarem seu objetivo primordial, que é o de regulamentar o comportamento do ser humano em sua vida cotidiana.

Assim, é importante que as abordagens políticas e tecnológicas para combater o crime cibernético sejam diversas e integradas. Só por meio de uma abordagem integrada e colaborativa que combina medidas legislativas, tecnológicas, educacionais e de cooperação internacional, podemos garantir um ambiente digital seguro e protegido para todos e mitigar os riscos relacionados ao cibercrime.

3.1. COMPREENDER AS TENDÊNCIAS DO CIBERCRIME

As tendências dos crimes cibernéticos estão em constante evolução, impulsionado pela rápida transformação digital e pela crescente sofisticação das tecnologias. Como resultado, novas tendências e padrões de comportamento surgem regularmente, desafiando as estratégias de segurança cibernética e exigindo respostas adaptativas por parte das organizações e autoridades.

Uma das tendências notáveis nos cibercrimes é o aumento da complexidade e sofisticação dos ataques, os criminosos estão cada vez mais adotando abordagens altamente técnicas e coordenadas, muitas das vezes utilizando-se de ferramentas avançadas, como *malware* modular e técnicas de evasão de detecção, para contornar as defesas tradicionais. Ademais, observa-se uma tendência em direção à especialização, como grupos criminosos organizados se dedicando a atividades específicas, como *ransomware*, fraude financeira ou espionagem.

Nesse sentido, o levantamento realizado e divulgado pela empresa de soluções de cibersegurança *Fortinet*, levando em conta os dados do *FortiGuard Labs,* aponta que o ataque do tipo *ransomware* segue em alta, uma vez que, cada vez mais os dados pessoais estão conectados ao ambiente virtual.

A pesquisa ainda mostra que em 2022, 82% dos crimes cometido na *internet* motivados financeiramente envolveram a utilização de *ransomware* e *scripts* maliciosos, o que mostra que esses ataques permanecem em pleno vigor, sem nenhum sinal de desaceleração, ainda mais com a popularização do *ransomware-as-a-Service* (RaaS) na *dark web* (negociação na qual desenvolvedores ransomware vendem seus *malware* para outros hackers).

A pesquisa ainda mostra uma aumento de 16% do volume de *ransomware* no segundo semestre de 2022, em comparação com o primeiro semestre do mesmo ano. A pesquisa visa mostrar que o levantamento divulgado aponta o Brasil como sendo o segundo país da América Latina mais atingido pelas tentativas de ataques cibernéticos em 2022, com um total de 103,16 bilhões de tentativas de ataques.

Outra tendência significativa é o crescimento de ataques direcionados e de estado-nação, os cibercriminosos estão cada vez mais mirando em alvos específicos, como grandes empresas, agências governamentais e infraestruturas críticas, em busca de dados sensíveis e sigilosos, propriedades intelectuais ou

influência política, observa-se um aumento nas atividades cibernéticas patrocinadas pelo estado, com governos empregando hackers para realizar espionagem, sabotagem ou guerras cibernéticas, cada vez mais comuns nos dias de hoje.

O surgimento de novas tecnologias e tendências, como inteligência artificial, também conhecida como IA, criptomoedas e outros, também tem impulsionado o cenário dos crimes cibernéticos. A IA está cada vez mais utilizada tanto por criminosos quanto por elementos defensores da segurança com a automatização de tarefas para identificar padrões e até mesmo desenvolver ataques personalizados. Além disso, as tensões geopolíticas e os conflitos entre países estão se alimentando de uma corrida armamentista digital, com investimentos crescentes em capacidades ofensivas e defensivas.

Pode-se dizer que as tendências do cibercrimes estão em constante evolução, refletindo os avanços tecnológicos, mudanças no cenário regulatório e geopolítico e a crescente sofisticação das ameaças.

3.2. PREVENÇÃO DOS ATAQUES CIBERNÉTICOS

A prevenção dos ataques cibernéticos é sem dúvida um dos pontos que mais necessitam de atenção em um mundo cada dia mais digitalizado, no qual as ameaças virtuais estão em constante evolução e aprimoramento. Para amortecer esses riscos e proteger os sistemas, dados e informações sensíveis e sigilosas, são necessárias estratégias abrangentes e proativas.

Um dos principais pilares da prevenção contra os ataques cibernéticos é a implementação de medidas de segurança robustas nos mais diversos níveis, desde o usuário individual até as grandes instituições e corporações governamentais, inclui a utilização de *firewalls*, antivirus, *software* de detecção de intrusões e autenticação multifatorial para proteger redes e dispositivos contra invasões e *malware.*

Nesse sentido existem diversos sites e blogs oferecem ideias para a proteção contra os crimes cibernéticos, como por exemplo, o *Security Leaders* aponta algumas estratégias de cibersegurança que todo *Chief Information Security Officers* (CISOs) ou empresas precisam investir em 2024:

a) Adoção da abordagem Zero *Trust* (Zero Confiança), que consiste na restrição de acessos a usuários ou dispositivos, sejam internos ou externos à

rede, que não possuem verificação.

b) Conformidade com regulamento de privacidade de dados, a aderência a normas globais e locais de proteção de informações sensíveis, como a LGPD.

c) Segurança da *internet* das coisas (IoT), Descreve a rede de objetos físicos incorporados a sensores, software e outras tecnologias com o objetivo de conectar e trocar dados com outros dispositivos. Com o crescimento da IoT, automaticamente tal campo passou a ser cada vez mais atacado.

d) Programas de Bug Bounty consiste na mobilização de uma comunidade de pesquisadores qualificados para identificar falhas antes mesmo que os cibercriminosos possam explorá-las.

Além disso, é crucial impulsionar a educação e conscientização sobre a segurança cibernética em todos os setores da sociedade, a sociedade deve ser informada sobre as melhores práticas de segurança, como a criação de senhas mais seguras, a atualização regular de *software* e o cuidado ao clicar em links suspeitos ou baixar arquivos de fontes desconhecidas.

Ademais, a elaboração de legislações específicas para os crimes cibernéticos é fundamental para a prevenção de ataques, isso inclui a definição clara de tipos de atividades criminosas online, como invasão de sistemas, roubo de dados e fraudes cibernéticas, bem como a imposição de penas proporcionais a esses crimes. Leis rigorosas e eficazes ajudam a dissuadir potenciais cibercriminosos e fornecem um arcabouço legal para a investigação e punição dos responsáveis por ataques cibernéticos.

Nesse sentido é válido citar a Portaria Nº 291, de 17 de dezembro de 2020, que institui o Comitê de Segurança Cibernética do Poder Judicial sobre a normatização para a criação do Centro de tratamento de Incidentes de Segurança Cibernética, que funciona como um canal oficial para orquestração de ações preventivas e corretivas, para os casos de ameaças ou ataques cibernéticos. O que evidencia que as normas brasileiras buscam meios para enfrentar os crimes cibernéticos.

A legislação relacionada à privacidade e proteção de dados desempenha um papel fundamental na prevenção de ataques cibernéticos. Leis como a Lei Geral de Proteção de Dados (LGPD) no Brasil estabelecem diretrizes para o tratamento de informações pessoais e impõem requisitos rigorosos para a coleta, armazenamento

e compartilhamento de dados. Ao garantir a proteção adequada das informações dos usuários, essas leis ajudam a reduzir os riscos de violações de dados e ataques de *phishing*. Vale ressaltar ainda, a importância da cooperação internacional e do compartilhamento de informações entre países, dada a natureza transnacional dos cibercrimes.

É essencial que as autoridades policiais e judiciárias de diferentes países trabalhem em conjunto para investigar e combater essas ameaças. Tratados e acordos internacionais de cooperação em matéria de cibercrime, como a Convenção de Budapeste do Conselho da Europa, facilitam o intercâmbio de dados e a assistência mútua entre os países na luta contra o crime cibernético.

É fundamental que os profissionais do direito saibam lidar com questões relacionadas à cibercriminalidade, isso significa que precisamos de uma atenção especial para a educação jurídica e conscientização sobre segurança cibernética. É essencial que os profissionais jurídicos entendam de direito digital e segurança da informação para entenderem as leis e as melhores práticas para lidar com crimes cibernéticos no sistema judicial.

A prevenção de ataques cibernéticos requer uma abordagem abrangente e coordenada, o que inclui a elaboração de leis eficazes, promover cooperação internacional, proteger a privacidade e educar os profissionais do direito. Somente através de um esforço coletivo, com autoridades, instituições jurídicas e a sociedade civil, é possível enfrentar de maneira efetiva as ameaças cibernéticas e garantir que o ambiente digital seja seguro e confiável para todos.

As informações lançadas na internet sempre devem ser verificadas de várias fontes, no intuito de determinar sua veracidade. A aplicação de ferramentas e procedimentos que possam detectar dados e informações falsas, no intuito de excluir imediatamente tais inverdades no meio virtual é uma alternativa que pode contribuir para minimizar práticas delituosas.

CONCLUSÃO

À medida que a sociedade avança rapidamente em direção a uma era cada vez mais digitalizada, os crimes cibernéticos emergem como uma ameaça persistente e multifacetada que afeta não apenas a segurança dos indivíduos, mas

também a integridade de instituições e sistemas vitais. Esta pesquisa buscou explorar os diversos aspectos dos crimes cibernéticos, desde suas origens e motivações até as medidas necessárias para mitigar seu impacto e prevenir futuros ataques.

No decorrer do trabalho uma das principais descobertas foi a complexidade e a evolução constante dos crimes cibernéticos, devido à natureza dinâmica e transfronteiriça do ambiente digital, com isso os criminosos estão sempre mudando suas formas e técnicas para explorar vulnerabilidades dos sistemas e redes.

A conscientização de como proteger-se online se torna cada vez mais importante para combater os crimes na *internet.* Educar os usuários finais sobre práticas seguras de computação e promover uma cultura de vigilância digital são passos essenciais para reduzir a exposição a ameaças cibernéticas. Além disso, a capacitação de profissionais do direito em questões relacionadas à cibercriminalidade e a promoção da cooperação internacional são fundamentais para fortalecer a capacidade de resposta legal e judicial diante dessas ameaças.

Os avanços da legislação tentam de todo modo minimizar os avanços da cibercriminalidade, contudo, como foi dito no decorrer do trabalho tais avanços estão em constante evolução e aperfeiçoamento, dificultando com que a legislação acompanhe e se antecipe às novas modalidades de cibercrimes.

Como foi visto a investigação de condutas ilícitas no ambiente virtual não é de fácil apuração, considerando a estrutura e o aparato estatal para as providências necessárias; à questão de descobrir os autores criminosos de fato que realizam ataques cibernéticos poderia ajudar a controlar, por exemplo, as transferências de dados dos usuários, por isso se faz necessário o investimento em leis específicas como a LGPD, para tratar da segurança nos ambientes virtuais que possam ajudam a aumentar a confiança dos usuários da *internet*.

Ao passo que avançamos para um futuro cada vez mais conectado, é imperativo que enfrentemos os desafios dos crimes cibernéticos com determinação e colaboração. Somente através de esforços coordenados e uma abordagem abrangente podemos proteger nossa infra estruturas digitais, garantir a segurança dos dados e promover um ambiente online seguro e confiável para todos os usuários.

REFERÊNCIAS

ARAS, Vladimir. *Crimes de informática. Uma nova criminalidade.* Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 6, n. 51, 1 out. 2001. Disponível em: https://jus.com.br/artigos/2250. Acesso em: 15 Novembro. 2023.

BRASIL. Constituição (1988). *Constituição da República Federativa do Brasil*. Brasília, DF: senado, 1988.

BRASIL. Decreto-Lei 2.848, de 07 de dezembro de 1940. Código Penal. Diário Oficial da União, Rio de Janeiro, 31 dez.

CONVENÇÃO DE BUDAPESTE, disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11491.htm . Acesso em : 19 de Novembro. 2023.

Crimes Cibernéticos, *Organização da Nações Unidas* (ONU), Disponível em: https://www.unodc.org/lpo-brazil/pt/covid19/cibercriminalidade-e-desinformacao.html. Acesso em: 19 de Novembro. 2023.

CUSTO ESTIMADO DO CRIME CIBERNÉTICO EM TODO O MUNDO 2017-2028. Disponível em: https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide. Acesso em 13 de março de 2024.

CONSELHO NACIONAL DE JUSTIÇA. PORTARIA Nº 291, DE 17 DE DEZEMBRO DE 2020.

CASSANTI, Moisés de Oliveira. Crimes Virtuais, Vítimas reais. Rio de Janeiro: Brasport, 2014.

ELEUTÉRIO, Pedro Monteiro da Silva; MACHADO, Marcio Pereira. Desvendando a Computação Forense. São Paulo: Novatec, 2011.

FORTINET, Fortiguard Labs. O BRASIL É SEGUNDO PAÍS MAIS ATINGIDO POR CIBERATAQUES NA AMÉRICA LATINA. Disponível em: https://febrabantech.febraban.org.br/temas/seguranca/brasil-e-segundo-pais-mais-atingido-por-ciberataques-na-america-latina-diz-relatorio. Acesso em 23 de março de 2024.

HENRIQUES, Antônio. Monografia no curso de direito: como elaborar o trabalho de conclusão de curso. 8. ed. São Paulo: Atlas, 2014.

JESUS, Damásio Evangelista de. Manual de Crimes Informáticos. 1ª ed. São Paulo: Saraiva, 2016.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. Fundamentos de metodologia científica. 7. ed. São Paulo: Atlas, 2010.

LEITE, Eduardo de Oliveira. A monografia jurídica. 9. ed. São Paulo: Revista dos Tribunais, 2001.

LISBOA, Roberto Senise. Direito na sociedade da informação. Disponível em: <https://www.academia.edu/42972871/DIREITO_NA_SOCIEDADE_DA_INFORMA%C3%87%C3%83O> Acesso em: 17 novembro. 2023.

O QUE É MALWARE. TECHTUDO, 2023. Disponível em: https://www.techtudo.com.br/listas/2021/03/o-que-e-malware-veja-significado-tipos-e-saiba-remover.ghtml. Acesso em: 22 novembro. 2023.

O QUE É HACKING?. KASPERSKY, 2023. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/what-is-hacking. Acesso em 22 novembro. 2023.

PHISHING: CONHEÇA OS PRINCIPAIS TIPOS. CONTACTA, 2023. Disponível em: https://www.contacta.com.br/phishing-conheca-os-principais-tipos/. Acesso em 22 novembro. 2023.

RELATÓRIO REVELA QUE 40% DOS CIBERCRIMES ENVOLVEM MANIPULAÇÃO PSICOLÓGICA. Disponível em: https://securityleaders.com.br/relatorio-revela-que-40-dos-cibercrimes-envolvem-manipulacao-psicologica/. Acesso em 23 de março de 2024.

ROSA, Fabrízio. Crimes de Informática. 2.ed. Campinas: BookSeller, 2006.

SIMAS, Diana Viveiros de. O cibercrime. 2014. 168f. Dissertação (Mestrado em Ciências Jurídico Forenses). Universidade Lusófona de Humanidades e Tecnologias. Lisboa. 2014.

SILVA, Patrícia Santos da. Direito e crime cibernético: análise da competência em razão do lugar no julgamento de ações penais. Brasília: Vestnik, 2015. Disponível em:<https://profmatheus.com/wp-content/uploads/2017/05/direito-crime cibernetico.pdf>

SILVA, Rita de Cássia Lopes. Direito penal e sistema informático. São Paulo: Revista dos Tribunais, 2003.

TIPOS DE PIRATARIA. VERITAS, 2023. Disponível em: https://www.veritas.com/pt/br/company/legal/anti-piracy/types-of-piracy. Acesso em: 22 novembro. 2023.