UNIVERSIDADE ESTADUAL DA PARAÍBA
CAMPUS I
CENTRO DE CIÊNCIAS JURÍDICAS
CURSO DE DIREITO

FABRÍCIO PIRES DE CARVALHO

CRIMES CIBERNÉTICOS: DESAFIOS LEGAIS E REGULAMENTARES ENTRE SEGURANÇA E PRIVACIDADE

CAMPINA GRANDE
2024

FABRÍCIO PIRES DE CARVALHO

CRIMES CIBERNÉTICOS: DESAFIOS LEGAIS E REGULAMENTARES ENTRE SEGURANÇA E PRIVACIDADE

Trabalho de conclusão de curso apresentado ao Centro de Ciências Jurídicas, Universidade Estadual da Paraíba, como requisito parcial para a obtenção do título de Bacharel em Direito.

Área de concentração: Ciências Criminais e novas tecnologias.

Orientadora: Prof. Dra. Ana Alice Ramos Tejo Salgado

CAMPINA GRANDE
2024

C331c Carvalho, Fabrício Pires de.
Crimes cibernéticos [manuscrito] : desafios legais e regulamentares entre segurança e privacidade / Fabricio Pires de Carvalho. - 2024.
20 p.

Digitado.
Trabalho de Conclusão de Curso (Graduação em Direito) - Universidade Estadual da Paraíba, Centro de Ciências Jurídicas, 2024.
"Orientação : Profa. Dra. Ana Alice Ramos Tejo Salgado, Coordenação do Curso de Direito - CCJ. "

1. Transformações tecnológicas. 2. Crimes cibernéticos. 3. Cibersegurança. I. Título

21. ed. CDD 345

Elaborada por Kênia O. de Araújo - CRB - 15/649 BSCCJ/UEPB

FABRÍCIO PIRES DE CARVALHO

CRIMES CIBERNÉTICOS: DESAFIOS LEGAIS E REGULAMENTARES ENTRE SEGURANÇA E PRIVACIDADE

Trabalho de conclusão de curso apresentado ao Centro de Ciências Jurídicas, Universidade Estadual da Paraíba, como requisito parcial para a obtenção do titulo de Bacharel em Direito.

Área de concentração: Ciências Criminais e novas tecnologias.

Aprovado em: 27/06/24.

BANCA EXAMINADORA

Ana Alice Ramos Tejo Salgado
Prof. Dra. Ana Alice Ramos Tejo Salgado (Orientadora)
Universidade Estadual da Paraíba (UEPB)

Esley Porto
Prof. Esley Porto
Universidade Estadual da Paraíba (UEPB)

Rayane Felix Silva
Prof. Rayane Felix Silva
Universidade Estadual da Paraíba (UEPB)

SUMÁRIO

CRIMES CIBERNÉTICOS: DESAFIOS LEGAIS E REGULAMENTARES ENTRE SEGURANÇA E PRIVACIDADE

Fabrício Pires de Carvalho [1*]
Ana Alice Ramos Tejo Salgado[2**]

RESUMO

A crescente dependência da internet para transações financeiras, comunicação e armazenamento de dados, tem tornado a cibercriminalidade uma preocupação global. O problema central se encontra na sofisticação e anonimato que essas tecnologias oferecem aos criminosos, dificultando a identificação e captura dos responsáveis. O tema deste artigo é crimes cibernéticos: desafios legais e regulamentares entre segurança e privacidade. Investigou o seguinte problema: Quais os desafios legais e regulamentares para manter a segurança e privacidade no mudo virtual? Cogitou-se a seguinte hipótese: a dificuldade de se fazer prova e investigar a origem do delito, a materialidade e a autoria dificulta o enfrentamento aos cibercrimes, como o atraso de leis e tratados específicos a respeito do tema na medida que a sociedade evolui dificulta o enfrentamento do problema. O objetivo geral é explorar os avanços legais sobre crimes cibernéticos no Brasil considerando as dificuldades investigativas e a linha tênue entre segurança e privacidade. Para tanto, tem-se como objetivos específicos definir crimes cibernéticos e analisar os desafios regulamentares na produção de provas e identificar os avanços nacionais em garantir segurança cibernética. Essa pesquisa é classificada como exploratória. Para viabilizar o estudo, foi realizado um levantamento bibliográfico utilizando as doutrinas conhecidas do direito brasileiro, jurisprudências e demais legislações. Conclui-se que os desafios legais e regulamentares entre segurança e privacidade continuam a ser um dilema significativo e que o equilíbrio entre esses dois aspectos é crucial para desenvolver uma abordagem eficaz e ética no combate aos crimes cibernéticos.

Palavras-chave: Transformações tecnológicas; Crimes cibernéticos; Cibersegurança; Desafios da etapa de investigação criminal.

[1*]Graduando em Bacharelado em Direito pela Universidade Estadual da Paraíba (UEPB). Endereço eletrônico: fabriciopiresdecarvalho@hotmail.com.
[2**]Graduada em Direito pela Universidade Estadual da Paraíba, doutorado pela Universidade Estadual do Rio de Janeiro. Docente UEPB e da Unifacisa na disciplina de Direito Penal. E-mail: anatejo@servidor.uepb.edu.br.

ABSTRACT

The growing dependence on the internet for financial transactions, communication and data storage has made cybercrime a global concern. The central problem lies in the sophistication and anonymity that these technologies offer to criminals, making it difficult to identify and capture those responsible. The theme of this article is cybercrimes: legal and regulatory challenges between security and privacy. Investigated the following problem: What are the legal and regulatory challenges to maintaining security and privacy in the virtual world? The following hypothesis was considered: the difficulty of proving and investigating the origin of the crime, the materiality and authorship makes it difficult to combat cybercrimes, as the delay in laws and specific treaties regarding the topic as society evolves makes it difficult tackling the problem. The general objective is to explore legal advances on cybercrimes in Brazil considering investigative difficulties and the fine line between security and privacy. To this end, the specific objectives are to define cybercrimes and analyze the regulatory challenges in producing evidence and identify national advances in ensuring cyber security. This research is classified as exploratory. To make the study viable, a bibliographical survey was carried out using known doctrines of Brazilian law, jurisprudence and other legislation. It is concluded that the legal and regulatory challenges between security and privacy continue to be a significant dilemma and that the balance between these two aspects is crucial to developing an effective and ethical approach to combating cybercrime.

Keywords: Technological transformations; Cyber crimes. Cybersecurity; Challenges of the criminal investigation stage;

1 INTRODUÇÃO

O presente trabalho, intitulado “Crimes cibernéticos: desafios legais e regulamentares entre segurança e privacidade”, tem como objetivo central analisar as dificuldades do processo investigatório e da produção probatória dos crimes cibernéticos. Considerando a linha tênue entre segurança e privacidade nos ambientes virtuais.

Os crimes cibernéticos vêm se expandindo na medida em que aumenta o acesso ao mundo virtual. Nessa linha, o Laboratório de segurança especializado em identificar ameaças digitais (Psafe Tecnologia S.A.), empresa de cibersegurança, apresentou dados que mostram o grau do problema enfrentado: no ano de 2021, provavelmente em razão da pandemia da covid-19, que impulsionou mais pessoas

para o trabalho em casa, houve um crescimento de 97% (noventa e sete por cento) dos ataques cibernéticos, em relação a 2020.

A regulamentação dos crimes cibernéticos no Brasil se deu pelo avanço da tecnologia, aumentando também as relações intermediadas por meio digital que encara uma crescente incidência de crimes virtuais no mundo, dado o aumento das ocorrências as medidas de regulamentação vieram com a finalidade de coibir a prática através da punição

Numa evolução cronológica, aponta-se a lei 12.737/2012 de 30 de novembro de 2012, conhecida como “Lei Carolina Dieckmann”, como o início de um conjunto de alterações legislativas que passam a tipificar como crimes ou agravar condutas praticadas no ambiente virtual.

A mais recente é a Lei 14155/2021 sancionada no dia 27 de maio de 2021, que tornou mais rigorosa a punição para os crimes de violação de dispositivo informático, furto e estelionato cometidos pela internet ou por meio de dispositivos eletrônicos, objetivando desestimular e reduzir o crescimento dos crimes cibernéticos.

Nesse contexto, discute-se a efetividade das regulamentações contra os crimes virtuais, haja vista o exponencial aumento desses casos, o despreparo e a deficiência de ferramentas para o enfrentamento do problema. Observa-se que tais regulamentações vêm se mostrando ineficientes. Diante dessa realidade, questiona-se: quais os desafios legais e regulamentares para manter a segurança e privacidade no mundo virtual?

Para responder a esse questionamento e considerando o aumento significativo de ataques, levanta-se a seguinte hipótese de que decorrem fatores, como: dificuldade de se fazer prova, de se investigar a origem do delito, a materialidade e a autoria dos cibercrimes; O despreparo dos profissionais responsáveis e a deficiência de ferramentas para investigação atrasando o trabalho do combate aos cibercrimes.

Isto posto, faz-se primordial empenhar o olhar sobre as regulamentações no enfrentamento aos crimes cibernéticos, analisando sua efetividade em reprimi-los, traduzindo suas fragilidades e possibilitando o fortalecimento das medidas de combate, trazendo mais segurança e confiabilidade para o meio digital.

O estudo sobre os crimes cibernéticos, desafios legais e regulamentares entre segurança e privacidade, trará benefícios significativos para a sociedade, aumentando o foco sobre o tema e alavancando a melhoria da segurança digital. Isso garantirá um ambiente online mais seguro para os cidadãos, empresas e instituições, ao mesmo tempo em que promoverá o desenvolvimento de expertise nacional nessa área, fortalecendo a capacidade de enfrentar os desafios futuros relacionados à segurança cibernética.

Investigar os desafios enfrentados no combate a esses crimes e analisar a legislação brasileira relacionada ao tema contribuirá para o desenvolvimento de novos conhecimentos e teorias nesta área.

Assim como oferece uma oportunidade de analisar a legislação brasileira existente e identificar suas limitações e lacunas no contexto dos crimes cibernéticos. Com base nesse conhecimento, é possível sugerir ajustes e melhorias na legislação,

visando garantir uma abordagem mais eficaz e abrangente para combater esses crimes, fortalecendo o sistema jurídico e adaptando-o às novas realidades digitais.

Por fim, beneficiará o combate à impunidade, uma vez que o entendimento dos desafios no combate aos crimes cibernéticos ajudará a desenvolver estratégias mais eficazes para a investigação e punição dos criminosos, envolvendo a cooperação entre diferentes instituições, como forças de segurança, órgãos judiciais e empresas de tecnologia. Dessa forma, o estudo contribuirá para o desenvolvimento de futuras estruturas normativas que efetivamente freiem a incidência dos crimes cibernéticos, com foco nas vítimas de crimes cibernéticos, operadores do Direito e sociedade em geral.

2 IMPACTOS DAS TRANSFORMAÇÕES SOCIAIS TECNOLÓGICAS E OS NOVOS CRIMES

Doutrinariamente, inexiste consenso acerca do conceito de crime cibernético, tendo sido utilizado para descrever como qualquer atividade ilícita praticada se utilizando da internet ou tecnologias digitais como meio principal. Esses crimes podem variar desde fraudes financeiras, roubo de identidade até invasão de sistemas e disseminação de malwares (código de software ou programa de computador intencionalmente escrito para prejudicar um sistema de computador ou seus usuários).

A crescente dependência da internet para transações financeiras, comunicação e armazenamento de dados, tem tornado a cibercriminalidade uma preocupação global. O problema central se encontra na sofisticação e anonimato que essas tecnologias oferecem aos criminosos, dificultando a identificação e captura dos responsáveis.

Nas décadas de 1980 e 1990, o Brasil vivenciou uma abertura positiva no âmbito econômico devido a influência do processo de globalização, que mostrava a necessidade de ser criada uma estrutura adequada para o desenvolvimento tecnológico do país (FIORILLO; CONTE, 2016).

Na medida que o Brasil investia em tecnologia, progressos significativos foram alcançados em áreas como telecomunicações, tecnologia da informação, biotecnologia e energias alternativas. Esses avanços ajudaram a melhorar a qualidade de vida do povo brasileiro, promovendo o desenvolvimento socioeconômico e a modernização da infraestrutura.

Com a expansão e reorganização do capitalismo após 1980, a sociedade se encaminha para uma grande transformação, que sob os aspectos da globalização, intensificou a industrialização. Em meio a mudanças e evoluções, houve a integralização da rede mundial de computadores e suas interconexões, que era uma das formas mais importantes de comunicação e difusão de dados e ideias. Assim, a sociedade passou a ser mais entendida ou representada, diante do impacto da internet e das relações interpessoais (PANNAIN; PEZZELLA, 2015).

Como muitas empresas começaram a investir em tecnologia, houve o aumento do fornecimento de dados dos usuários e a partir disso, tais informações eram arquivadas e facilmente rastreáveis por meio dos algoritmos. Por conseguinte, ainda nos meados da década de 1980, com as novas transformações no âmbito

social e econômico, houve um aumento de ações criminosas, que começaram a se refletir em manipulações de caixas bancários, pirataria de programa e pornografia infantil, abusos de telecomunicação e demais fatores que começaram preocupar os cidadãos (OLIVEIRA JÚNIOR, 2013).

A Constituição Federal de 1988 incluiu em capítulo próprio o direito à segurança pública. A segurança pública é o direito social que permite

> O direito à segurança, espécie de direito social, traz para o Estado o dever de implementar políticas públicas de segurança que garantam aos cidadãos o direito de ir, vir e transitar com tranquilidade nos locais públicos e, também, assegurem a defesa de sua integridade física e de seu patrimônio. O direito à segurança é parte fundamental do direito à qualidade de vida e do próprio direito fundamental à vida, na medida em que a insegurança traz aumento de violência e perturbação à ordem pública e social (Ferrer, 2007, p. 109).

Nesse sentido, o combate aos crimes cibernéticos também é imprescindível. No entanto, com o surgimento constante de novas formas de lesar o direito em uma nova realidade, engajou as empresas em investir na segurança dos usuários e seus dados, assim também como foram redigidas novas tipificações nos Códigos e leis brasileiras, garantindo a proteção dos usuários de tecnologia digital ou eletrônica.

Conforme os autores Jesus e Milagre (2016, p. 9), os crimes cibernéticos também podem ser conhecidos como crimes virtuais, que se refere a ‘’fatos típicos e antijurídicos cometidos por meio da, ou contra a tecnologia da informação, ou seja, um ato típico e antijurídico, cometido através da informática em geral’’.

O autor Rocha (2017, p. 13), explica que os crimes cibernéticos trata-se de condutas ilícitas realizadas por algum tipo de dispositivo tecnológico (Qualquer aparelho que utilize tecnologia digital ou eletrônica para funcionar.), (...), por entender-se que as realizações das condutas são dadas em um ambiente virtual’’.

Ainda assim, o mesmo jurista destaca que os crimes cibernéticos são divididos como crimes próprios e crimes impróprios. O primeiro é definido por condutas antijurídicas e culpáveis, tendo como principal objetivo de prejudicar um sistema ou violar dados, e nos crimes impróprios são as comuns, que também são antijurídicas e culpáveis, podendo ser realizado fora do ambiente virtual, que transgride os direitos da privacidade, à honra, intimidade e até mesmo contra a imagem.

Contudo, é perceptível que a legislação brasileira para frear os crimes cibernéticos não acompanhou tal evolução, pois a cada dia que se passa, vão surgindo novos tipos de práticas ilegais no mundo virtual, no qual às vezes não se pode punir os infratores por falta de leis específicas ou da ineficácia do sistema judiciário em achar o criminoso.

A investigação e produção de provas em casos de cibercrimes apresenta desafios. A natureza transnacional desses crimes, onde as atividades ilícitas podem ocorrer em um país e afetar vítimas em outro, exige cooperação internacional e uma compreensão profunda das tecnologias envolvidas. Além disso, para a preservação e a análise de evidências digitais requerem técnicas forenses especializadas que garantirão a admissibilidade das provas em juízo. Esses procedimentos incluem a captura de dados em tempo real, rastreamento de atividades online e análise de logs de servidores, tudo enquanto se mantém a integridade das evidências coletadas.

Assim, a eficácia no combate à cibercriminalidade depende não só de uma legislação robusta, mas também de capacitação técnica e cooperação global entre as autoridades.

O Brasil está entre os cinco países do mundo que mais usam internet, conforme Organização para a Cooperação e Desenvolvimento Econômico (OCDE), (Gov.br, 2022). Por conseguinte, na proporção que os números progridem, os ciberataques aumentaram drasticamente nos últimos anos, pois é relativamente fácil para os criminosos ocultar sua localização e identidade, sendo, portanto, essencial que os usuários da internet estejam atentos para que não sejam vítimas de tais atos.

3 CIBERCRIMES: DESAFIOS LEGAIS E REGULAMENTARES ENTRE SEGURANÇA E PRIVACIDADE

Os crimes cibernéticos podem assumir diversas formas, duas são comumente praticadas: crimes que visam atacar computadores seja para obter informações, chantagear vítimas ou causar danos a terceiros ou crimes que visam utilizar computadores para outras atividades ilegais. Em casos assim, os dispositivos e redes funcionam como ferramentas criminosas.

Na legislação brasileira, muitos desses crimes cibernéticos são tipificados para garantir a proteção dos cidadãos contra atividades ilícitas no ambiente digital. A fraude por e-mail e usando a Internet, por exemplo, é abordada pela Lei nº 14.155/2021. De acordo com o Art. 171, § 2º-A do Código Penal, a pena para estelionato é aumentada se o crime for cometido mediante a utilização de informação fornecida pela vítima ou por terceiros induzidos a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento. Isso visa combater os golpes que se espalham rapidamente por esses meios.

O roubo de dados financeiros ou credenciais bancárias de terceiros, sejam indivíduos ou organizações, também é rigorosamente tratado. A Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, tipificada no Art. 154-A do Código Penal a invasão de dispositivo informático alheio para obter, adulterar ou destruir dados ou informações sem autorização, incluindo dados financeiros. Adicionalmente, a mesma lei prevê a difusão de vírus informático como crime no Art. 154-B, punindo a produção, oferta, distribuição, venda ou difusão de programas de computador que possam causar danos a dispositivos informáticos.

A invasão de computadores pessoais, de empresas ou redes de computadores é igualmente punida sob o Art. 154-A do Código Penal, conforme a Lei nº 12.737/2012. Este artigo penaliza a invasão de dispositivo informático alheio, conectado ou não à rede de computadores, com o objetivo de obter, adulterar ou destruir dados ou informações, ou instalar vulnerabilidades para obter vantagem ilícita. Extorsão cibernética e ransomware, onde criminosos exigem resgate para devolver o acesso a dados criptografados, são enquadrados no Art. 158 do Código Penal, que trata da extorsão mediante violência ou grave ameaça para obter vantagem econômica indevida.

Crimes como o phishing, comuns em golpes disseminados pelas redes sociais e aplicativos de mensagens, são abordados pela Lei nº 14.155/2021. No Art. 171, § 2º-A do Código Penal, a lei aumenta a pena para estelionato quando a fraude é cometida por meio eletrônico. Além disso, o cryptojacking, que envolve a utilização

não autorizada de dispositivos alheios para mineração de criptomoedas, é tipificado pela mesma Lei nº 12.737/2012, no Art. 154-A, como invasão de dispositivo informático para instalar software de mineração.

A violação de direitos autorais é tipificada pela Lei nº 9.610/1998 (Lei de Direitos Autorais) no Art. 184 do Código Penal, punindo a violação de direitos de autor e conexos. Jogos de azar ou ilegais em território nacional são tratados pelo Decreto-Lei nº 3.688/1941, no Art. 50, que aborda contravenções penais relacionadas ao estabelecimento ou exploração de jogos de azar em locais públicos ou acessíveis ao público. A venda de itens ilegais pela internet, como drogas, é tratada pela Lei nº 11.343/2006 no Art. 33, que criminaliza o tráfico de drogas.

A incitação, produção ou posse de pornografia infantil é rigorosamente punida pelo Estatuto da Criança e do Adolescente, Lei nº 8.069/1990, em seus artigos 241 a 241-E. Já o discurso de ódio, incluindo publicações de teor homofóbico, xenófobo, racista e apologia ao nazismo, é tratado pela Lei nº 7.716/1989. O Art. 20 e o Art. 20-A dessa lei criminalizam a discriminação e a incitação ao ódio com base em raça, cor, etnia, religião ou procedência nacional, e a jurisprudência do STF equipara a homofobia e transfobia ao crime de racismo. A apologia ao nazismo é especificamente abordada pelo Art. 20, § 1º da mesma lei, que proíbe a fabricação, comercialização e veiculação de símbolos nazistas.

É claro que novas oportunidades para tais crimes surgem em todas as fases do desenvolvimento da sociedade, e o sistema judiciário deve estar sempre atento aos fatos. Em relação à Lei nº 12.965/2014, também conhecida como Marco Civil da Internet, assegura em conjunto com seus dispositivos uma série de direitos e deveres relacionados ao uso da Internet no Brasil, estabelecendo princípios, garantias, direitos e deveres para o uso da internet no país.

A Lei nº 12.965/2014 estabelece, entre outras coisas, a proteção à privacidade dos usuários, a neutralidade da rede e a responsabilidade dos provedores de conexão e aplicação pela proteção dos dados pessoais dos usuários. Ela obriga os provedores de serviços a manterem registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e seguro, por um prazo determinado. Além disso, estabelece que esses registros só podem ser fornecidos mediante ordem judicial.

Outro ponto importante é que o Marco Civil da Internet determina que a liberdade de expressão, a comunicação e a manifestação do pensamento são garantidas e que a exclusão de conteúdos somente pode ocorrer mediante ordem judicial, exceto em casos específicos, como a nudez e pornografia de menores.

A Lei nº 12.965/2014 também atua como um instrumento de combate aos crimes cibernéticos, pois fornece uma base legal sólida para a obtenção de provas digitais e a cooperação internacional em investigações. Ela estabelece que o acesso à internet é essencial ao exercício da cidadania e que todos têm direito à privacidade e à proteção de seus dados pessoais.

Diante do andamento legislativo, Jesus e Milagre comentou sobre o Marco Civil:

> Recentemente, quando deixávamos um serviço na internet, não sabíamos se efetivamente os provedores apagavam nossos dados. Em muitos casos era cediço, embora excluíssemos nossas contas, nossos dados permaneciam

> disponíveis ou armazenados. Com o Marco Civil, o usuário poderá requerer a exclusão definitiva de seus dados pessoais fornecidos a uma aplicação de internet, e o provedor deverá atender, ressalvados, logicamente, os dados que deva guardar por disposição legal. (JESUS, MILAGRE, 2014, p. 36).

Esses dispositivos reforçam a necessidade de uma vigilância constante e de uma atualização contínua das leis para acompanhar o rápido avanço tecnológico e as novas modalidades de crimes cibernéticos que surgem.

Mesmo diante do volume de texto legal existente, as denúncias de crimes virtuais ainda aumentam, de acordo com Alessandro Di Lorenzo, para o TechTudo (2024), a pesquisa da Check Point Research, o Brasil registrou 38% de aumento nos ciberataques em geral no primeiro trimestre deste ano. Mostrando que os esforços não vêm sendo suficientes para afugentar a ação criminosa. Desse modo o internauta deve estar atento, buscando conhecer as mazelas do mundo virtual para evitar que se torne vítima.

Os crimes cibernéticos representam um desafio crescente em uma era cada vez mais digitalizada, onde a proteção da segurança e da privacidade dos indivíduos e organizações se torna cada vez mais complexa. A velocidade com que novas tecnologias e métodos de ataque são desenvolvidos frequentemente supera a capacidade dos legisladores e reguladores de criar e atualizar leis. Isso cria lacunas jurídicas que os criminosos podem explorar, tornando a evolução tecnológica rápida um dos principais obstáculos na luta contra o cibercrime.

A investigação e a produção de provas em casos de cibercrimes apresentam desafios. A natureza transnacional desses crimes, onde as atividades ilícitas podem ocorrer em um país e afetar vítimas em outro, exige cooperação internacional e uma compreensão profunda das tecnologias envolvidas. Além disso, para a preservação e análise de evidências digitais requerem técnicas forenses especializadas que garantirão a admissibilidade das provas em juízo. Esses procedimentos incluem a captura de dados em tempo real, rastreamento de atividades online e análise de logs de servidores, tudo enquanto se mantém a integridade das evidências coletadas. Assim, a eficácia no combate à cibercriminalidade depende não só de uma legislação robusta, mas também de capacitação técnica e cooperação global entre as autoridades.

Leis como o GDPR (Regulamento Geral sobre a Proteção de Dados) na Europa impõem severas restrições sobre como os dados pessoais devem ser coletados, armazenados e processados. Isso afeta a forma como as investigações cibernéticas podem ser conduzidas, especialmente no que diz respeito à coleta de evidências digitais. As empresas de tecnologia, como provedores de serviços de internet e plataformas de mídia social, muitas vezes são pressionadas a colaborar com investigações criminais e a fornecer dados de usuários. Ainda assim, essas empresas também têm a responsabilidade de proteger a privacidade dos usuários, criando um dilema ético e legal significativo.

Encontrar um equilíbrio entre segurança e privacidade é um dos maiores desafios no combate aos crimes cibernéticos. Segurança implica em medidas preventivas e reativas robustas contra atividades criminosas, incluindo vigilância, monitoramento e análise de dados em larga escala. Contudo, tais medidas podem infringir a privacidade dos indivíduos, levando a abusos e vigilância em massa. Por outro lado, a privacidade envolve a proteção dos dados pessoais e a garantia de que

as informações dos indivíduos não sejam acessadas ou usadas sem consentimento. Todavia, uma ênfase excessiva na privacidade pode limitar a capacidade das autoridades de investigar e prevenir crimes cibernéticos eficazmente.

Para solucionar esses desafios, é essencial desenvolver acordos e normas internacionais que harmonizem a definição e a abordagem dos crimes cibernéticos, facilitando a cooperação e a aplicação da lei entre países. Fortalecer a colaboração entre governos e empresas privadas para compartilhar informações e desenvolver tecnologias de segurança cibernética que respeitem a privacidade também é crucial. A implementação de tecnologias de privacidade preservadoras, como criptografia homomórfica e aprendizado de máquina com preservação de privacidade, pode permitir a análise de dados e a detecção de ameaças sem comprometer a privacidade dos indivíduos.

Os crimes cibernéticos representam um desafio significativo tanto em termos legais quanto regulamentares. O equilíbrio entre segurança e privacidade requer uma abordagem multifacetada, envolvendo a atualização constante das leis, a colaboração internacional e o desenvolvimento de novas tecnologias que respeitem os direitos dos indivíduos.

Além disso, promover a educação e conscientização sobre segurança cibernética entre usuários e profissionais é fundamental para que possam proteger melhor suas informações e entender os riscos envolvidos. A combinação dessas abordagens pode ajudar a criar um ambiente digital mais seguro e justo para todos.

3.1 Crimes cibernéticos e desafios da etapa de investigação criminal

Mesmo com o estabelecimento de muitas normas para limitar as atividades nocivas no mundo virtual, são identificadas várias lacunas que ainda precisam ser preenchidas pelo legislador, pois em um mundo onde recursos imensuráveis e ferramentas infinitas podem ser obtidos, é importante que tal ordem possa lidar com situações onde, por exemplo, um alvo pode desaparecer no ciberespaço porque então seria muito fácil para um usuário criar uma conta falsa e imediatamente danificar a reputação dessa pessoa e então deletar a conta depois de todas as consequências.

Destaca-se assim Jesus e Milagre (2016):

> Entretanto, a progressiva mutação tecnológica dificulta o combate a esses crimes, que estão em constante alinhamento com as novas tecnologias. Assim, com o uso incontido e indiscriminado da internet, alguns indivíduos com conhecimento em informática passaram a se aprimorar e utilizar esses conhecimentos para roubar informações criptografadas, como já havia sido feito há muito tempo, para obter proveito econômico ou ainda, por mera diversão. (JESUS e MILAGRE, 2016)

Em alguns casos, ainda é possível identificar o responsável, mas o ainda teria que apresentar todo o processo para comprovar tal atividade. Segundo Fernando Tourinho Filho (2009) entendimento da veracidade do fato:

> Antes de mais nada, estabelecer a existência da verdade; e as provas são os meios pelos quais se procura estabelecê-la. É demonstrar a veracidade do que se afirma, do que se alega. Entendem-se, também, por prova, de ordinário, os elementos produzidos pelas partes ou pelo próprio Juiz visando a estabelecer, dentro do processo, a existência de certos fatos. É o instrumento de verificação do thema probandum. (TOURINHO, 2009, P. 522).

Em 2015, a Comissão Parlamentar de Inquérito (CPI) do Brasil, com membros, destacou as grandes dificuldades em rastrear, detectar e punir crimes online. A Agência Câmara de Notícias (2015) relatou dificuldades em encontrar a pessoa responsável pelos crimes:

> A dificuldade se deve ao fato de que a velocidade de obter as informações com as empresas não ocorre na velocidade da internet. O chefe do Serviço de Repressão a Crimes Cibernéticos da PF, Elmer Vicente, explicou que a investigação começa com a identificação do endereço IP do computador de onde partiu o crime, que é dado pelo provedor de serviço. O próximo passo é conseguir, com o provedor de internet, o nome do usuário do IP. Segundo Elmer, no entanto, há duas grandes dificuldades. A primeira é que, curiosamente, algumas empresas não aceitam a requisição de informações da polícia pela internet. Outra dificuldade é que, se antes algumas empresas concediam informações por meio de requisição policial, com o marco civil da internet, as empresas geralmente cedem os dados apenas por meio judicial. (AGÊNCIA CÂMARA DE NOTÍCIAS, 2015)

Assim como as pessoas possuem números de identificação como o CPF (Cadastro de Pessoa Física), os computadores e periféricos conectados à Internet também possuem números que são separados de um endereço IP por serem o número único do protocolo que permite o acesso de máquinas à rede (SALGA BRAGA, 2018).

Vale lembrar que nem todos os cibercriminosos são especializados ou experientes na área de informática. Alguns desses crimes, como crimes contra a honra, podem ser cometidos por usuários comuns com apenas um celular ou qualquer dispositivo técnico com conexão à internet, essas situações podem ser mais fáceis de identificar.

Por outro lado, usuários que cometem crimes virtuais podem utilizar as chamadas máscaras online para ocultar suas identidades, o que ainda é uma questão relevante. Isso torna impossível determinar a localização e a identidade reais do criminoso. Em resumo, a função de uma máscara web é simular que o dispositivo está em um local diferente da cena do crime. Por exemplo, um crime cometido em Brasília, Brasil, pode parecer ter sido realizado a partir da China, graças à falsificação de um endereço IP. Esse mecanismo dificulta a obtenção de evidências pelos especialistas em investigação.

Além disso, é necessário que a sociedade em geral realize um levantamento abrangente da Internet, para que o usuário conheça as armadilhas de crimes e abusos, de maneiras a evitá-los e, ao mesmo tempo, a capacidade de lutar contra

tais violações. Ao mesmo tempo, o Estado também deve tentar se antecipar a esses criminosos, treinar seus agentes para que os responsáveis sejam encontrados e restaurar a ordem social.

3.2 Desenvolvimento de estratégias nacionais de cibersegurança

O Brasil tem desenvolvido estratégias nacionais de cibersegurança, buscando garantir a proteção de seus sistemas digitais, essas estratégias residem na capacidade de fornecer uma abordagem abrangente para lidar com ameaças cibernéticas. Ao alinhar suas estratégias com diretrizes internacionais, os países podem aproveitar as melhores práticas globais, promovendo a interoperabilidade e a cooperação internacional. Essa adesão a padrões comuns fortalece a resiliência cibernética, permitindo respostas mais eficazes a incidentes e uma maior capacidade de recuperação.

Outro ponto forte é a ênfase na conscientização e na promoção de uma cultura de segurança cibernética. Estratégias nacionais frequentemente incluem medidas para educar cidadãos, empresas e setor público sobre as ameaças digitais e as melhores práticas de segurança. Isso contribui para criar uma população mais informada e vigilante, reduzindo o potencial de sucesso de ataques cibernéticos.

No entanto, os desafios também são evidentes no desenvolvimento dessas estratégias. Um dos pontos fracos é a rápida evolução do cenário cibernético, o que pode tornar as estratégias desatualizadas em curtos períodos. As ameaças digitais estão em constante mutação, exigindo uma adaptação constante das estratégias para lidar com novos vetores de ataque.

Outro desafio reside na necessidade de equilibrar a segurança cibernética com a privacidade individual e a liberdade na internet. Medidas robustas de segurança podem, por vezes, entrar em conflito com direitos individuais, levantando questões éticas e jurídicas complexas. Encontrar esse equilíbrio é crucial para garantir que as estratégias não comprometam inadvertidamente outros valores fundamentais.

Além disso, a implementação efetiva das estratégias é frequentemente afetada pela falta de recursos, tanto financeiros quanto humanos. Garantir a eficácia das políticas de cibersegurança requer investimentos contínuos em treinamento, tecnologia e pessoal qualificado, o que pode ser um desafio em contextos de recursos limitados.

As estratégias nacionais de cibersegurança apresentam pontos fortes, como a adoção de padrões internacionais e a promoção da conscientização, mas também enfrentam desafios, incluindo a rápida evolução do cenário cibernético e a necessidade de equilibrar a segurança com outros valores sociais. Abordar esses desafios é fundamental para garantir uma resposta eficaz às ameaças cibernéticas em constante evolução.

4 METODOLOGIA

A metodologia descreve os procedimentos de coleta e análise de dados e materiais que levam aos resultados (MOTA-ROTH; HENDGES; 2010). O método de pesquisa utilizado é qualitativo e baseado em técnicas de coleta de dados. Segundo Neves (1996, p. 01), o objetivo da pesquisa qualitativa não é listar ou mensurar eventos. Serve informações descritivas que expressam os significados dos fenômenos.

Essa pesquisa é classificada como exploratória, fornecendo informações adicionais sobre o assunto em questão, além de ser classificada como uma cadeia de raciocínio usando o método dedutivo, que a partir de teorias e leis gerais pode acabar determinando ou predizendo certos fenômenos. (MARCONI e LAKATOS, 2017).

Para viabilizar o estudo, foi realizado um levantamento bibliográfico utilizando as doutrinas conhecidas do direito brasileiro, jurisprudências e demais legislações que regulam a relação entre os crimes cibernéticos, a lacuna em torno deles. a codificação dessas atividades ilícitas no ordenamento jurídico brasileiro e seus possíveis problemas perante a lei e a sociedade.

5 CONCLUSÃO

Buscou-se explorar os impactos das transformações sociais e tecnológicas que revelam a complexidade e a urgência de enfrentar os crimes cibernéticos em um mundo cada vez mais digitalizado. Observou-se que a evolução tecnológica, embora tenha proporcionado inúmeros benefícios socioeconômicos, também abriu caminho para novos desafios no campo da segurança digital. Identificou-se também que a sofisticação e o anonimato que essas tecnologias oferecem aos criminosos dificultam a identificação e captura dos responsáveis, evidenciando a necessidade de uma legislação adaptada e eficaz.

Esta pesquisa demonstrou o avanço tecnológico desde a década de 1980 que impulsionou significativas melhorias nas áreas de telecomunicações e tecnologia da informação. Contudo, a mesma expansão que trouxe progresso também facilitou o aumento de crimes cibernéticos, desde fraudes financeiras até invasões de sistemas e disseminação de malwares. Mostrando, assim, que a legislação brasileira, apesar de ter evoluído, ainda luta para acompanhar a rápida inovação tecnológica, muitas vezes falhando em punir adequadamente os criminosos virtuais devido a lacunas legais e desafios na coleta de provas.

O Direito Penal avançou com os processos evolutivos da sociedade, alcançou significativamente regulações para os denominados crimes digitais, incluindo leis específicas como a Lei Carolina Dieckmann e o Marco Civil da Internet, estabeleceu marcos importantes na proteção dos dados e na responsabilização dos infratores. Contudo, trouxe a luz que a eficácia dessas leis depende não apenas de sua robustez, mas também da capacitação técnica das autoridades e da cooperação

internacional. A transnacionalidade dos crimes cibernéticos exige uma colaboração global para garantir a segurança digital e a proteção dos cidadãos.

Esta pesquisa demonstrou que os desafios legais e regulamentares entre segurança e privacidade continuam a ser um dilema significativo. A necessidade de proteger a privacidade dos indivíduos frequentemente entra em conflito com as medidas de segurança cibernética necessárias para prevenir e investigar crimes. Identificando que o equilíbrio entre esses dois aspectos é crucial para desenvolver uma abordagem eficaz e ética no combate aos crimes cibernéticos.

Destacou-se, ainda, que a criação de estratégias nacionais de cibersegurança no Brasil representa um passo importante na proteção contra ameaças digitais. Estratégias estas, que alinhadas com diretrizes internacionais, enfatizam a conscientização e a educação sobre segurança cibernética, contribuindo para uma população mais informada e vigilante.

Conclui-se, portanto, que a luta contra os crimes cibernéticos exige uma abordagem multifacetada que inclua legislação atualizada, capacitação técnica, cooperação internacional e um equilíbrio cuidadoso entre segurança e privacidade. Somente através de esforços coordenados e contínuos será possível criar um ambiente digital seguro e justo para todos. A sociedade e o Estado devem estar em constante vigilância e adaptação para enfrentar as novas ameaças, garantindo a proteção dos direitos dos cidadãos e a integridade das informações no mundo virtual.

REFERÊNCIAS

BRAGA, Diego Campos Salgado. **Métodos de investigações no âmbito cibernético**. Jus.com.br, novembro de 2018. Disponível em: <https://jus.com.br/artigos/71463/metodos-de-investigacoes-no-ambito-cibernetico>. Acesso em: 28 nov. 2022.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Planalto**. Brasília. 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 27 nov. 2022.

_____. Lei n° 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei n° 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências. **Diário Oficial da União**, Brasília, 30 nov. 2012.

CANUTO, Luiz Cláudio. **CPI constata dificuldade em rastrear e punir crimes de internet**. Câmara dos Deputados. agosto de 2015. Disponível em: <https://www.camara.leg.br/noticias/467819-cpi-constata-dificuldade-em-rastrear-e-punir-crimes-de-internet/> . Acesso em: 28 nov. 2022.

Di Lorenzo, Alessandro. Ciberataques no Brasil aumentam 38% no primeiro trimestre de 2024. Disponível em: https://olhardigital.com.br/2024/04/22/seguranca/ciberataques-no-brasil-aumentam-38-no-primeiro-trimestre-de-2024/. Acesso em: 04 de jun. 2024.

FERRER, Flávia. O Direito à Segurança. Revista do Ministério Público. Rio de Janeiro: MPRJ, n. 26, jul./dez. 2007

FIORILLO, Celso Antonio Pacheco; CONTE, Christiany Pegorari. **Crimes no meio ambiente digital**. 2. ed., São Paulo: Saraiva, 2016.

FONSECA, Marcos De Lucca ; GENNARINI, Juliana Caramigo. A Adesão do Brasil à Convenção de Budapeste e os Impactos Para a Produção de Provas Digitais. Revista de Direito Penal e Processo Penal, ISSN 2674-6093, v. 4, n. 1, jan./jun. 2022.

GARRETT, Filipe. Crimes cibernéticos**:** entenda o que são e como denunciar. **Techtudo**, agosto de 2021. Disponível em: <https://www.techtudo.com.br/noticias/2021/08/crimes-ciberneticos-entenda-o-que-sao-e-como-denunciar.ghtml>. Acesso em: 24 nov. 2022.
Gov.br, 17/04/2023. Convenção de Budapeste é promulgada no Brasil. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/convencao-de-budapeste-e-promulgada-no-brasil#:~:text=Bras%C3%ADlia%2C%2017%2F04%2F2023,Crime%20Cibern%C3%A9tico%2C%20firmada%20em%20Budapeste. Acesso em: 06 de jun. de 2024.

Gov.br, 31/10/2022. Brasil está entre os cinco países do mundo que mais usam internet. Disponível em:https://www.gov.br/pt-br/noticias/transito-e-transportes/2021/04/brasil-esta-entre-os-cinco-paises-do-mundo-que-mais-usam-internet#:~:text=ENTREVISTA-,Brasil%20est%C3%A1%20entre%20os%20cinco%20pa%C3%ADses%20do%20mundo%20que%20mais%20usam%20internet,-Pa%C3%ADs%20participou%20de. Acesso em: 31 de mai. de 2024.

Grossmann, Luís Osvaldo. Brasil adere formalmente à Convenção de Budapeste sobre cibercrime. Disponível em: https://www.convergenciadigital.com.br/Seguranca/Brasil-adere-formalmente-a-Convencao-de-Budapeste-sobre-cibercrime-62973.html?UserActiveTemplate=mobile. Acesso em 17 de jun. 2024.

JESUS, Damásio de. MILAGRE, José Antonio. **Manual de crimes de informáticos.** São Paulo: Saraiva, 2016.

_____. **Marco Civil da Internet:** Comentário à Lei 12.965/14. São Paulo: Saraiva, 2014.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Fundamentos de metodologia Científica**, 8. ed., Atlas, 2017.

MOTTA-ROTH, Désirée; HENDGES, Graciela H. **Produção textual na universidade**. São Paulo: Parábola Editorial, 2010.

NEVES, J. L. **Pesquisa qualitativa:** características, usos e possibilidades. Caderno de pesquisa em administração. V. 1., n° 3., 1996.

OLIVEIRA JÚNIOR, Eudes Quitino de. **A nova lei Carolina Dieckmann**. Disponível em:. <https://eudesquintino.jusbrasil.com.br/artigos/121823244/a-nova-lei-carolina-dieckmann>. Acesso em: 24 nov. 2022.

PANNAIN, Camila Nunes; PEZZELLA, Maria Cristina. Liberdade de Expressão e Hate Speech na Sociedade da Informação. **Revista Direitos Emergentes da Sociedade Global**. Santa Maria, v. 4, N°1, 2015.

ROSA, Fabrízio. **Crimes de informática**. 2. ed., Campinas: Bookseller, 2006.

ROCHA, Adriano Aparecido. **Cibercriminalidade**: os crimes cibernéticos e os limites da liberdade de expressão na internet. São Paulo, 2017. Disponível em:<https://www.faef.br/userfiles/files/23%20-%20CIBERCRIMINALIDADE%20E%20OS%20LIMITES%20DA%20LIBERDADE%20DE%20EXPRESSAO%20NA%20INTERNET.pdf. Acesso em 27 nov. 2022.

Superior Tribunal de Justiça - AgRg no HC: 611724 DF 2020/0232683-4, Relator: Ministro JOÃO OTÁVIO DE NORONHA, Data de Julgamento: 17/11/2020, T5 - QUINTA TURMA, Data de Publicação: Diário de justiça eletrônico 20/11/2020. Disponível em: <https://www.jusbrasil.com.br/jurisprudencia/stj/1206243333>. Acesso em: 27 nov. 2022.

TOURINHO FILHO, Fernando da Costa. **Manual de processo penal**. 12.ed., São Paulo: Saraiva, 2009.

AGRADECIMENTOS

Agradeço, ao criador de todas as coisas, por ter me conduzido até aqui, nunca deixando que me faltasse a fé e a coragem. Com amor e mais puro carinho àquela que me deu a vida, minha mãe, pela dedicação, companheirismo, cuidado e pela pessoa de minha mais profunda admiração, a quem procuro me inspirar. A minha irmã que sempre me apoiou, com uma palavra amiga.

Meus sinceros agradecimentos também aos meus familiares que me apoiaram desde minha chegada na cidade de Campina Grande até os dias de hoje. Dedico este trabalho também à minha companheira, Pâmella Victória Soares Lima, pelos conselhos, apoio moral e palavras sábias que me foram transmitidas.

Ao Centro de Ciências Jurídicas da Universidade Estadual da Paraíba (UEPB), campus I, Campina Grande, e corpo docente os quais tive o privilégio de ter como mestres e que me apoiaram sempre na minha caminhada.

Em especial a querida professora, Ana Alice Ramos Tejo Salgado, pela sábia orientação e colaboração, bem como à professora Aureci Gonzaga Farias, que em muito contribuiu para a elaboração do Projeto de Pesquisa que iniciou o presente trabalho.