INTERNATIONAL SEVEN JOURNAL
OF MULTIDISCIPLINARY
ISSN: 2764-9547

Desafios jurídicos e técnicos na perseguição de criminosos cibernéticos: Uma análise das dificuldades enfrentadas pelas autoridades

Legal and technical challenges in the pursuit of cybercriminals: An analysis of the difficulties faced by the authorities

DOI: 10.56238/isevmjv2n5-015
Recebimento dos originais: 18/09/2023
Aceitação para publicação: 06/10/2023

Erik Richardson Faria e Sousa

RESUMO
A rápida expansão da tecnologia da informação e comunicação tem gerado um cenário digital em constante crescimento, onde a internet e as redes digitais desempenham um papel central. No entanto, essa ubiquidade tecnológica trouxe consigo desafios, como os crimes cibernéticos sofisticados e em constante evolução. Este artigo aborda a complexidade e diversidade dos crimes cibernéticos, suas implicações legais e as dificuldades enfrentadas pelas autoridades para identificar e punir os infratores. A pesquisa se baseia em uma abordagem qualitativa, apoiada por revisão bibliográfica, para explorar as nuances da prevenção e combate a esses crimes. As lacunas na legislação específica exigem que o sistema jurídico se adapte e atualize constantemente. Tecnologias como análise forense digital, rastreamento de IP e segurança cibernética têm sido usadas tanto por autoridades quanto por criminosos. A colaboração e a constante evolução das estratégias de combate são essenciais para enfrentar essa realidade em mutação na era digital.

Palavras-chave: Crimes cibernéticos, Legislação, Tecnologia, Segurança cibernética, Investigação.

1 INTRODUÇÃO

A rápida expansão da tecnologia da informação e comunicação na sociedade contemporânea tem delineado um cenário digital em constante crescimento. Nesse contexto, a internet e as redes digitais desempenham um papel central, permeando praticamente todas as esferas das nossas vidas. No entanto, essa ubiquidade tecnológica não apenas traz benefícios, mas também coloca desafios diante do sistema jurídico, dado o surgimento de crimes cibernéticos cada vez mais sofisticados e complexos.

Os crimes cibernéticos, com seu caráter transnacional e em constante evolução, apresentam desafios únicos tanto para a sociedade quanto para as autoridades legais incumbidas de combatê-los. Ao contrário dos crimes convencionais, a natureza virtual dessas infrações permite que os perpetradores ajam a distância, muitas vezes no anonimato. A facilidade de ocultar a identidade, aliada à constante inovação de técnicas, tem impulsionado o crescimento exponencial dessas ameaças cibernéticas (NASCIMENTO, 2016).

A ausência de uma legislação específica para lidar efetivamente com os crimes cibernéticos faz com que o sistema jurídico existente seja adaptado para essa finalidade. A definição precisa e a categorização dos tipos de crimes cibernéticos são tarefas complexas, dada a sua natureza altamente técnica e em constante evolução. A necessidade de atualização constante das leis e regulamentos para acompanhar as táticas em mutação dos cibercriminosos adiciona pressão adicional às autoridades legais (Aquino Junior, 2014).

Este artigo, motivado pela urgência de compreender os desafios que o sistema jurídico enfrenta, busca explorar as nuances da prevenção e combate aos crimes cibernéticos. O núcleo desta pesquisa reside na investigação das dificuldades que as autoridades enfrentam na identificação e punição dos responsáveis por essas infrações.

A metodologia adotada é a pesquisa qualitativa, que visa captar a complexidade em constante mutação dos crimes cibernéticos (Para isso, a pesquisa bibliográfica, conforme definida por Lakatos e Marconi (2017), desempenha um papel crucial, fornecendo o arcabouço teórico necessário para situar o tema, identificar lacunas no conhecimento e fundamentar a relevância da pesquisa.

Por meio de uma análise abrangente, este artigo visa lançar luz sobre as diversas dimensões dos crimes cibernéticos, avaliar a eficácia das abordagens legais atuais e propor possíveis soluções para um enfrentamento mais eficiente dessas ameaças na era digital. Ao compreender melhor a complexidade desses crimes e os obstáculos que surgem no seu combate, espera-se que a sociedade e os sistemas jurídicos estejam mais preparados para lidar com essa realidade em constante evolução.

2 DESENVOLVIMENTO

2.1 CONCEITOS BÁSICOS DE CRIMES CIBERNÉTICOS

A cibernética engloba os sistemas informantes e os sistemas de informação, oferecendo uma abordagem ampla e apropriada. Sob o prisma do conceito analítico finalista de crime, os crimes cibernéticos abrangem ações típicas, antijurídicas e culpáveis cometidas por meio de sistemas informáticos, abarcando não somente invasões e roubos de dados, mas também variadas atividades fraudulentas e prejudiciais facilitadas pela tecnologia (TORMEN, 2018).

> No mundo, dois em cada três usuários já foram vítimas de crimes virtuais, que atingem 556 milhões de pessoas todos os anos. Só no Brasil, o prejuízo anual é o maior de todos, estimado em R$ 16 bilhões. Os dados são de 2012, da empresa de segurança virtual Symantec. De acordo com o relatório de 2014 da Kaspersky Lab, outra companhia de segurança na Internet, o Brasil é o segundo país onde mais acontecem fraudes bancárias. (TECMUNDO, 2016)

Santos (2021) em seu estudo comenta que os crimes cibernéticos compreendem atividades ilícitas executadas por meio de tecnologias da informação e internet. Isso abrange desde invasões a sistemas (hacking) e tentativas de obtenção de informações confidenciais (phishing), até a disseminação de malware prejudicial, como ransomware, e o assédio online (cyberbullying). Além disso, crimes financeiros, como fraudes em cartões de crédito e ciberespionagem para obtenção de informações estratégicas, também são componentes desse cenário. A variedade desses crimes demonstra a complexidade e a constante evolução das táticas empregadas por criminosos, exigindo esforços contínuos de conscientização, educação e segurança cibernética para enfrentar essas ameaças.

Os crimes cibernéticos abrangem uma ampla gama de atividades ilegais que se aproveitam da tecnologia digital, representando um desafio complexo e em constante evolução. Desde fraudes online que visam enganar indivíduos desavisados até ataques sofisticados de malware que podem paralisar infraestruturas críticas, essas ações prejudicam a segurança de sistemas, a privacidade das pessoas e a confiança nas transações online (NASCIMENTO, 2016).

A falta de uma legislação específica para tratar das questões relativas aos crimes cibernéticos atribui ao sistema penal atual a responsabilidade de julgar aqueles que praticam essas atividades ilícitas. Conforme revelado por uma pesquisa realizada pelo site Safernet, diversos crimes cibernéticos se destacam, incluindo pirataria, pornografia infantil, calúnia, difamação, injúria e estelionato, entre outros (SANTOS; MARTINS; TYBUCSH, 2017). Nesse vácuo normativo, o ordenamento jurídico vigente é convocado a lidar com os desafios desses delitos, destacando a necessidade de atualização e adaptação das leis às complexidades do ambiente digital.

A diversidade de crimes cibernéticos é notável, abrangendo desde invasões de sistemas até fraudes financeiras, passando por assédio online e disseminação de malware prejudicial. O cenário é marcado pela sofisticação das táticas empregadas pelos cibercriminosos, exigindo esforços contínuos de conscientização, educação e segurança cibernética, À medida que a tecnologia continua a avançar e a sociedade se torna cada vez mais dependente do mundo digital, os crimes cibernéticos provavelmente continuarão a evoluir em termos de sofisticação e escala. (TORMEN, 2018).

2.2 LEGISLAÇÃO RELACIONADA À CIBERCRIME

No cenário brasileiro, o crescente aumento dos crimes cibernéticos emerge como uma preocupação inquietante, como claramente demonstrado pelos dados da Fortinet (OLIVEIRA,

2022), que registram um notável incremento nas tentativas de ataques cibernéticos direcionados a empresas. Essas estatísticas acentuam a imperatividade de aprimorar as estratégias de enfrentamento e prevenção desses delitos, enquanto simultaneamente se reforça a segurança digital em todas as esferas. Nesse contexto, a presente pesquisa adota uma abordagem qualitativa, fazendo uso do levantamento bibliográfico como metodologia central de coleta de informações.

O artigo 5º, XXXIX, da Constituição Federal estabelece o princípio fundamental de que não pode haver crime sem uma lei anterior que defina claramente o seu enquadramento, assim como não pode haver pena sem uma previsão legal prévia. Isso significa que, para que uma conduta seja considerada criminosa e sujeita a penalidades, é necessário que exista uma lei que a descreva como tal antes da ocorrência do fato.

Esse princípio se aplica aos crimes cibernéticos da mesma forma que a qualquer outro tipo de crime. Portanto, se não houver uma tipificação penal específica para os crimes cibernéticos na legislação, tais condutas não serão consideradas crime e não estarão sujeitas a punições. Um exemplo relevante é a Lei 12.737/12, que é uma legislação que aborda explicitamente os Crimes Cibernéticos no Brasil. Essa lei é fundamental para estabelecer as bases legais para a criminalização e a punição de atividades ilícitas que envolvem o uso indevido da tecnologia e sistemas de informação.

No Brasil, de acordo com D'urso (2017) o ordenamento jurídico relacionado aos crimes digitais engloba diversas leis e regulamentos que abordam diferentes aspectos dessas infrações. Destacam-se o Marco Civil da Internet, o Código Penal, a Lei Carolina Dieckmann (ou "Lei dos Crimes Cibernéticos"), a Lei de Interceptações Telefônicas, a Lei de Lavagem de Dinheiro, a Lei de Combate ao Crime Organizado e a Lei Geral de Proteção de Dados. Essas leis abordam invasões de dispositivos, violações de privacidade, fraudes eletrônicas, crimes contra a honra, lavagem de dinheiro e outras práticas delituosas no ambiente digital, proporcionando um arcabouço legal para enfrentar os desafios dos crimes cibernéticos no país

O Marco Civil da Internet (Lei Nº 12.965/14) emerge como um marco regulatório que estabelece direitos e deveres tanto para os usuários quanto para os provedores de serviços relacionados ao uso da Internet. Paralelamente, a lei Carolina Dieckmann (Lei Nº 12.737/12) desempenha um papel significativo ao tipificar os crimes informáticos, inaugurando esforços iniciais para estabelecer uma base de segurança jurídica para as interações na esfera digital. No entanto, à medida que os crimes cibernéticos evoluem em sofisticação e escala, a adequação e atualização dessas leis se tornam essenciais.

A transnacionalidade dessas ofensas, aliada à facilidade de operação a partir de locais distantes, muitas vezes torna difícil a aplicação eficaz das leis nacionais. Além disso, a rápida mutação das táticas e técnicas empregadas pelos cibercriminosos exige que tanto as leis quanto às tecnologias de combate se adaptem constantemente para enfrentar essas ameaças em constante evolução. Diante deste cenário preocupante, as leis brasileiras têm se empenhado em proteger tanto o bem individual quanto o coletivo no ambiente digital (CERT. br, 2012).

2.3 TECNOLOGIAS E FERRAMENTAS UTILIZADAS NO COMBATE.

No campo do combate aos crimes cibernéticos, a tecnologia também se destaca como uma ferramenta de dupla natureza. Por um lado, é uma aliada essencial para as autoridades, permitindo rastrear, identificar e capturar infratores que operam no ambiente digital. Ferramentas de análise forense digital, técnicas de rastreamento de IP e softwares de segurança desempenham um papel crucial na investigação desses crimes. Por outro lado, os avanços tecnológicos também têm sido explorados por cibercriminosos para orquestrar ataques cada vez mais sofisticados, exigindo um constante aprimoramento das medidas de segurança cibernética. (D'URSO, 2017)

A abordagem proposta por Pisa (2012) para a análise dos cabeçalhos dos pacotes de informação revela-se um recurso indispensável na investigação de crimes cibernéticos. Através da minuciosa inspeção desses elementos, como endereços IP de origem, destinos e dados temporais, os investigadores podem traçar as rotas percorridas pelos dados em uma rede digital. Esse processo não apenas permite a identificação da localização geográfica aproximada do dispositivo utilizado para cometer o crime, mas também oferece uma visão mais completa das conexões, padrões e possíveis vínculos que podem levar à identificação do autor do delito.

No cenário em constante evolução dos crimes cibernéticos, o combate a essas ameaças demanda a utilização de um conjunto diversificado de tecnologias e ferramentas. Entre essas, destacam-se os firewalls e antivírus, fundamentais para a proteção de sistemas e redes contra invasões e malware, assim como sistemas de detecção e prevenção de intrusões (IDS/IPS), capazes de monitorar o tráfego em tempo real e responder rapidamente a atividades suspeitas. Além disso, a criptografia se revela essencial para garantir a segurança na transmissão de dados, preservando a confidencialidade e a integridade das informações sensíveis (CARDOSO, 2023).

A forense digital, por sua vez, oferece ferramentas vitais para coletar e analisar evidências em casos de incidentes cibernéticos, fornecendo suporte crucial para investigações legais. A análise de malware possibilita uma compreensão aprofundada das características e origens de códigos maliciosos, contribuindo para a identificação de vulnerabilidades exploradas.

Paralelamente, as plataformas de gerenciamento de incidentes de segurança (SIEM) centralizam informações provenientes de diversas fontes, permitindo a coordenação eficaz da detecção e resposta a ameaças (CARNEIRO, 2012).

A colaboração entre entidades é para Cardoso (2023) uma pedra angular no enfrentamento dos crimes cibernéticos, promovendo a troca de informações e o compartilhamento de inteligência sobre tendências e ameaças emergentes. O uso de inteligência artificial e aprendizado de máquina ganha destaque por sua capacidade de analisar grandes volumes de dados em tempo real, identificando padrões e comportamentos suspeitos que muitas vezes passariam despercebidos aos olhos humanos. Em conjunto, essas tecnologias e ferramentas representam uma estratégia multifacetada e em constante adaptação para combater as ameaças crescentes no cenário digital.

3 CONCLUSÃO

Em um mundo cada vez mais digitalizado e interconectado, os crimes cibernéticos se tornaram uma ameaça presente e em constante evolução. A expansão da tecnologia da informação e comunicação trouxe consigo inúmeras possibilidades, mas também desafios significativos para o sistema jurídico. A natureza virtual e transnacional dessas infrações tem desafiado a capacidade das autoridades legais de identificar, investigar e punir os responsáveis.

A ausência de uma legislação específica para crimes cibernéticos tem colocado a carga de adaptar o sistema jurídico existente para lidar com essa realidade em rápida mutação. A complexidade técnica desses crimes, aliada à necessidade de atualização constante das leis, exerce pressão adicional sobre as autoridades legais para manter-se atualizadas e eficazes.

A legislação brasileira tem buscado abordar essa problemática por meio de leis como o Marco Civil da Internet e a Lei dos Crimes Cibernéticos. No entanto, a transnacionalidade dos crimes e a rápida evolução tecnológica demandam uma constante adaptação e aprimoramento das leis e regulamentos. A tecnologia, por sua vez, atua como aliada e desafio nesse contexto. Ferramentas de análise forense digital, rastreamento de IP, softwares de segurança e técnicas de criptografia têm sido fundamentais na investigação e prevenção dos crimes, mas também são exploradas pelos próprios cibercriminosos

REFERÊNCIAS

AQUINO JUNIOR, G. F. de. RESPONSABILIDADE CIVIL NA INTERNET. Revista de Direito Constitucional e Internacional | vol. 86/2014 | p. 451 - 473 | Jan - Mar / 2014. Doutrinas Essenciais de Dano Moral | vol. 1/2015 | p. 451 - 473 | Jul / 2015. DTR\2015\9886.

BRASIL, Constituição Federal. Brasília, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 10 de agosto de 2023

BRASIL. Lei Nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 1º dez. 2012. Seção 1, p. 1.

BRASIL. Lei Nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 24 abr. 2014. Seção 1, p. 5.

CARDOSO, W. C. S. Evolução Tecnológica no Direito Penal e Crimes Cibernéticos: Technological Evolution in Criminal Law and Cyber Crimes. Belo Horizonte, 2023. Disponível em: <https://repositorio.animaeducacao.com.br/bitstream/ANIMA/34858/1/CENTRO%20UNIVERSITA%CC%81RIO%20DE%20BELO%20HORIZONTE%20-%20%28UNIBH%29.pdf>. Acesso em: 10 de agosto de 2023.

CARNEIRO, A. G. Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação. 2012. Âmbito Jurídico. Disponível em: https://ambitojuridico.com.br/edicoes/revista-99/crimes-virtuais-elementos-para-umareflexaosobreoproblemanatipificacao/#:~:text=Na%20d%C3%A9Cada%20de%2070%20a,%C3%A0%20dade%20de%20se%20despender. Acesso em: 10 de agosto de 2023

CERT.br. Cartilha de Segurança para Internet, versão 4.0 / Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) – São Paulo: Comitê Gestor da Internet no Brasil (CGI.br), 2012. Disponível em: https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf . Acesso em: Acesso em 14 de julho de 2023

D'URSO, L. A. F. Cibercrime: perigo na internet. Publicado em 2017. Disponível em https://politica.estadao.com.br/blogs/fausto-macedo/cibercrime-perigo-nainternet/ Acesso em 14 de julho de 2023

LAKATOS E; MARCONI E. A. Fundamentos da metodologia cientifica. ed. Atlas, 2017

NASCIMENTO, N. L. Crimes Cibernéticos. Fundação Educacional do Município de Assis – FEMA – Assis, 2016. 34 folhas. Disponível em: https://cepein.femanet.com.br/BDigital/arqTccs/1311401614.pdf. Acesso em: 28 de junho de 2023

OLIVEIRA, Ingrid. Levantamento mostra que ataques cibernéticos no Brasil cresceram 94%. CNN Brasil, [S.l.], 19 ago. 2022. Disponível em:

https://www.cnnbrasil.com.br/tecnologia/levantamento-mostra-que-ataques-ciberneticos-no-brasil-cresceram-94/#:~:text=Levantamento%20mostra%20que%20ataques%20cibern%C3%A9ticos%20no%20Brasil%20cresceram%2094%25,-Pa%C3%ADs%20%C3%A9%20o&text=O%20Brasil%20registrou%20no%20primeiro,16%2C2%20bilh%C3%B5es%20de%20registros.. Acesso em: 14 de julho de 2023

PISA, P. O que é IP? Copyright© Globo Comunicações e Participações S.A. techtudo, publicado em: 07 mai. 2012. Disponível em:https://www.techtudo.com.br/noticias/2012/05/o-que-e-ip.ghtml . Acesso em 14 de julho de 2023

SANTOS, A. C. dos. Crimes Cibernéticos. Monografia de Especialização, apresentada ao Curso de Especialização em Arquitetura e Gestão de Infraestrutura de TI, do Departamento Acadêmico de Eletrônica - DAELN, da Universidade Tecnológica Federal do Paraná - UTFPR, como requisito parcial para obtenção do título de Especialista. Orientador: Prof. Dr. Kleber Kendy Horikawa Nabas. Curitiba, 2021. Disponível em: https://repositorio.utfpr.edu.br/jspui/bitstream/1/29004/1/CT_CEGATI_I_2021_01.pdf . Disponível em: 14 de julho de 2023

SANTOS, L. R.; MARTINS, L. B.; TYBUCSH, F. B. A. Os crimes cibernéticos e o direito à segurança jurídica: uma análise da legislação vigente no cenário brasileiro contemporâneo. In: CONGRESSO INTERNACIONAL DE DIREITO E CONTEMPORANEIDADE, 4., 2017, Santa Maria, RS. Anais... Santa Maria: UFSM, 2017. Disponível em: http://www.ufsm.br/congressodireito/anais. Acesso em: 10 ago. 2023.

TECMUNDO. Crime Virtual: o que é e como se proteger das ameaças. 2016. Disponível em: https://www.tecmundo.com.br/crime-virtual/97401-crime-virtual-proteger-ameacas.htm . Acesso em: 10 de agosto de 2023