INTERNATIONAL SEVEN JOURNAL
OF MULTIDISCIPLINARY
ISSN: 2764-9547

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

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

DOI: 10.56238/isevmjv2n5-015
Receipt of originals: 18/09/2023
Acceptance for publication: 06/10/2023

Erik Richardson Faria e Sousa

ABSTRACT

The rapid expansion of information and communication technology has shaped a continually growing digital landscape, wherein the internet and digital networks play a central role. However, this technological ubiquity has brought forth challenges, such as sophisticated and ever-evolving cybercrimes. This article addresses the complexity and diversity of cybercrimes, their legal implications, and the difficulties authorities face in identifying and prosecuting offenders. The research employs a qualitative approach, supported by literature review, to explore the nuances of preventing and combating these crimes. Gaps in specific legislation necessitate constant adaptation and updates within the legal system. Technologies such as digital forensic analysis, IP tracking, and cybersecurity have been utilized by both authorities and criminals. Collaboration and the continuous evolution of counter-strategies are vital to confronting this ever-changing reality in the digital age.

Keywords: Cybercrimes, Legislation, Technology, Cybersecurity, Investigation.

1 INTRODUCTION

The rapid expansion of information and communication technology in contemporary society has outlined an ever-growing digital landscape. In this context, the internet and digital networks play a central role, permeating virtually all spheres of our lives. However, this technological ubiquity not only brings benefits, but also poses challenges in the face of the legal system, given the emergence of increasingly sophisticated and complex cybercrimes.

Cybercrime, with its transnational and constantly evolving character, presents unique challenges for both society and the legal authorities in charge of combating them. Unlike conventional crimes, the virtual nature of these offenses allows perpetrators to act from a distance, often anonymously. The ease of concealing one's identity, combined with the constant innovation of techniques, has driven the exponential growth of these cyber threats (NASCIMENTO, 2016).

The absence of specific legislation to effectively deal with cybercrime means that the existing legal system has been adapted for this purpose. Accurately defining and categorizing the types of cybercrime is a complex task, given its highly technical and ever-evolving nature. The need for constantly updating laws and regulations to keep up with cybercriminals' changing tactics adds additional pressure to legal authorities (Aquino Junior, 2014).

This article, motivated by the urgency of understanding the challenges facing the legal system, seeks to explore the nuances of preventing and combating cybercrime. The core of this research lies in the investigation of the difficulties that authorities face in identifying and punishing those responsible for these infractions.

The methodology adopted is qualitative research, which aims to capture the ever-changing complexity of cybercrime (To this end, bibliographic research, as defined by Lakatos and Marconi (2017), plays a crucial role, providing the theoretical framework necessary to situate the topic, identify gaps in knowledge, and substantiate the relevance of research.

Through a comprehensive analysis, this article aims to shed light on the various dimensions of cybercrime, evaluate the effectiveness of current legal approaches, and propose possible solutions for a more efficient confrontation of these threats in the digital age. By better understanding the complexity of these crimes and the obstacles that arise in combating them, it is hoped that society and legal systems will be better prepared to deal with this ever-evolving reality.

2 DEVELOPMENT

2.1 CYBERCRIME BASICS

Cybernetics encompasses both informant systems and information systems, offering a broad and appropriate approach. From the perspective of the finalist analytical concept of crime, cybercrimes encompass typical, anti-legal and culpable actions committed through computer systems, encompassing not only invasions and theft of data, but also various fraudulent and harmful activities facilitated by technology (TORMEN, 2018).

> Worldwide, two out of three users have been victims of cybercrime, which affects 556 million people every year. In Brazil alone, the annual loss is the largest of all, estimated at R$ 16 billion. The data is from 2012, from the cybersecurity company Symantec. According to a 2014 report by Kaspersky Lab, another Internet security company, Brazil is the second most common country for bank fraud. (TECMUNDO, 2016)

Santos (2021), in his study, comments that cybercrimes comprise illicit activities carried out through information technologies and the internet. This ranges from system intrusions (hacking) and attempts to obtain sensitive information (phishing), to the spread of harmful malware such as ransomware and online harassment (cyberbullying). In addition, financial crimes, such as credit card fraud and cyberespionage to obtain strategic information, are also components of this scenario. The variety of these crimes demonstrates the complexity and constant evolution of tactics employed by criminals, requiring ongoing awareness, education, and cybersecurity efforts to address these threats.

Cybercrime encompasses a wide range of illegal activities that take advantage of digital technology, posing a complex and ever-evolving challenge. From online scams that aim to deceive unsuspecting individuals to sophisticated malware attacks that can paralyze critical infrastructure, these actions undermine system security, people's privacy, and trust in online transactions (NASCIMENTO, 2016).

The lack of specific legislation to address issues related to cybercrime gives the current penal system the responsibility of prosecuting those who engage in these illicit activities. As revealed by a survey carried out by the Safernet website, several cybercrimes stand out, including piracy, child pornography, slander, defamation, slander and embezzlement, among others (SANTOS; MARTINS; TYBUCSH, 2017). In this normative vacuum, the current legal system is called upon to deal with the challenges of these crimes, highlighting the need to update and adapt laws to the complexities of the digital environment.

The diversity of cybercrime is remarkable, ranging from system intrusions to financial fraud to online harassment and the spread of harmful malware. The landscape is marked by the sophistication of tactics employed by cybercriminals, requiring ongoing awareness, education, and cybersecurity efforts, As technology continues to advance and society becomes increasingly reliant on the digital world, cybercrime will likely continue to evolve in terms of sophistication and scale. (TORMEN, 2018).

2.2 LEGISLATION RELATED TO CYBERCRIME

In the Brazilian scenario, the growing increase in cybercrime emerges as a worrying concern, as clearly demonstrated by Fortinet data (OLIVEIRA, 2022), which records a notable increase in attempted cyberattacks targeting companies. These statistics accentuate the imperative of improving strategies for coping with and preventing these crimes, while simultaneously reinforcing digital security in all spheres. In this context, the present research adopts a qualitative approach, making use of the bibliographic survey as a central methodology for collecting information.

Article 5, XXXIX, of the Federal Constitution establishes the fundamental principle that there can be no crime without a previous law that clearly defines its framework, just as there can be no penalty without a prior legal provision. This means that, in order for a conduct to be considered criminal and subject to penalties, it is necessary that there is a law that describes it as such before the fact occurs.

This principle applies to cybercrime in the same way as it does to any other type of crime. Therefore, if there is no specific criminal classification for cybercrimes in the legislation, such conduct will not be considered a crime and will not be subject to punishment. A relevant example is Law 12.737/12, which is a piece of legislation that explicitly addresses Cybercrime in Brazil. This law is essential to establish the legal basis for the criminalization and punishment of illicit activities that involve the misuse of technology and information systems.

In Brazil, according to D'urso (2017), the legal system related to digital crimes encompasses several laws and regulations that address different aspects of these offenses. Highlights include the Brazilian Civil Rights Framework for the Internet, the Penal Code, the Carolina Dieckmann Law (or "Cybercrime Law"), the Telephone Interception Law, the Money Laundering Law, the Law to Combat Organized Crime, and the General Data Protection Law. These laws address device intrusions, privacy violations, electronic fraud, crimes against honor, money laundering, and other criminal practices in the digital environment, providing a legal framework to address the challenges of cybercrime in the country

The Brazilian Civil Rights Framework for the Internet (Law No. 12,965/14) emerges as a regulatory framework that establishes rights and duties for both users and service providers related to the use of the Internet. At the same time, the Carolina Dieckmann law (Law No. 12,737/12) plays a significant role in criminalizing computer crimes, inaugurating initial efforts to establish a legal basis for interactions in the digital sphere. However, as cybercrime evolves in sophistication and scale, adapting and updating these laws becomes essential.

The transnationality of these offences, coupled with the ease of operation from distant locations, often makes it difficult to enforce national laws effectively. In addition, the rapidly changing tactics and techniques employed by cybercriminals require both laws and combat technologies to constantly adapt to meet these ever-evolving threats. Faced with this worrisome scenario, Brazilian laws have been committed to protecting both the individual and the collective good in the digital environment (CERT. br, 2012).

2.3 TECHNOLOGIES AND TOOLS USED IN COMBAT.

In the field of combating cybercrime, technology also stands out as a tool of dual nature. On the one hand, it is an essential ally for the authorities, allowing them to track, identify and capture offenders operating in the digital environment. Digital forensic analysis tools, IP tracking techniques, and security software play a crucial role in the investigation of these crimes. On the other hand, technological advances have also been exploited by cybercriminals to orchestrate increasingly sophisticated attacks, requiring a constant improvement of cybersecurity measures. (D'URSO, 2017)

The approach proposed by Pisa (2012) for the analysis of the headers of information packets proves to be an indispensable resource in the investigation of cybercrimes. Through thorough inspection of these elements, such as source IP addresses, destinations, and temporal data, investigators can trace the routes taken by data on a digital network. Not only does this process allow for the identification of the approximate geographic location of the device used to commit the crime, but it also provides a more complete view of the connections, patterns, and potential links that can lead to the identification of the offender.

In the ever-evolving landscape of cybercrime, combating these threats requires the use of a diverse set of technologies and tools. Among these, firewalls and antiviruses stand out, which are essential for protecting systems and networks against intrusions and malware, as well as intrusion detection and prevention systems (IDS/IPS), capable of monitoring traffic in real time and responding quickly to suspicious activities. In addition, encryption is essential to ensure security in data transmission, preserving the confidentiality and integrity of sensitive information (CARDOSO, 2023).

Digital forensics, meanwhile, offers vital tools for collecting and analyzing evidence in cases of cyber incidents, providing crucial support for legal investigations. Malware analysis enables an in-depth understanding of the characteristics and origins of malicious code, contributing to the identification of exploited vulnerabilities. At the same time, security incident management (SIEM) platforms centralize information from various sources, allowing for effective coordination of threat detection and response (CARNEIRO, 2012).

For Cardoso (2023), collaboration between entities is a cornerstone in the fight against cybercrime, promoting the exchange of information and the sharing of intelligence on emerging trends and threats. The use of artificial intelligence and machine learning stands out for its ability to analyze large volumes of data in real-time, identifying suspicious patterns and behaviors that would often go unnoticed by human eyes. Taken together, these technologies and tools represent a multifaceted and ever-adapting strategy to combat the growing threats in the digital landscape.

3 CONCLUSION

In an increasingly digitized and interconnected world, cybercrime has become a present and ever-evolving threat. The expansion of information and communication technology has brought with it numerous possibilities, but also significant challenges for the legal system. The virtual and transnational nature of these offences has challenged the ability of law enforcement authorities to identify, investigate and punish those responsible.

The absence of specific legislation for cybercrime has placed the burden of adapting the existing legal system to deal with this rapidly changing reality. The technical complexity of these crimes, coupled with the need for laws to be constantly updated, puts additional pressure on legal authorities to stay up-to-date and effective.

Brazilian legislation has sought to address this issue through laws such as the Brazilian Civil Rights Framework for the Internet and the Cybercrime Law. However, the transnationality of crimes and the rapid technological evolution demand a constant adaptation and improvement of laws and regulations. Technology, in turn, acts as an ally and challenge in this context. Digital forensic analysis tools, IP tracking, security software, and encryption techniques have been instrumental in investigating and preventing crimes, but they are also exploited by cybercriminals themselves

REFERENCES

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