III CONGRESSO INTERNACIONAL DE DIREITO, POLÍTICAS PÚBLICAS, TECNOLOGIA E INTERNET

DIREITO PENAL E CIBERCRIMES II

D598
Direito penal e cibercrimes II [Recurso eletrônico on-line] organização III Congresso Internacional de Direito, Políticas Públicas, Tecnologia e Internet: Faculdade de Direito de Franca – Franca;

Coordenadores: Renan Posella Mandarino, Fábio Cantizani Gomes e Ana Carolina de Sá Juzo – Franca: Faculdade de Direito de Franca, 2025.

Inclui bibliografia
ISBN: 978-65-5274-364-0
Modo de acesso: www.conpedi.org.br em publicações
Tema: Governança, regulação e o futuro da inteligência artificial.
1. Direito. 2. Políticas Públicas. 3. Tecnologia. 4. Internet. I. III Congresso Internacional de Direito, Políticas Públicas, Tecnologia e Internet (1:2025 : Franca, SP).

CDU: 34

III CONGRESSO INTERNACIONAL DE DIREITO, POLÍTICAS PÚBLICAS, TECNOLOGIA E INTERNET

DIREITO PENAL E CIBERCRIMES II

Apresentação

Entre os dias 30 de setembro e 3 de outubro de 2025, a Faculdade de Direito de Franca recebeu o III Congresso Internacional de Direito, Políticas Públicas, Tecnologia e Internet. O evento reuniu acadêmicos, profissionais, pesquisadores e estudantes, promovendo o debate interdisciplinar sobre o impacto das inovações tecnológicas no campo jurídico e nas políticas públicas. A programação envolveu Grupos de Trabalho (GTs) organizados para aprofundar temas específicos, abordando desde o acesso à justiça até as complexidades da regulação tecnológica, com ênfase na adaptação do sistema jurídico aos avanços da inteligência artificial e da automação.

O GT 9 foca nos crimes digitais e na responsabilização penal de condutas praticadas em ambiente virtual. As pesquisas discutem pornografia não consentida, cyberbullying, discursos de ódio e a eficácia das investigações digitais. O grupo ressalta a necessidade de adequação legislativa e de políticas públicas voltadas à prevenção e repressão dos cibercrimes.

CIBERCRIME E DIREITO: UMA ANÁLISE DOS DESAFIOS DA SEGURANÇA NA INTERNET

THE EVOLUTION AND COMBAT OF CYBER CRIMES: A LEGAL AND TECHNICAL ANALYSIS

Thainan Tammy Tameirão
Gisele da Silva Santos

Resumo

A globalização e a evolução tecnológica transformaram a forma como a informação é compartilhada e protegida. Com a crescente utilização da internet, surgem novos tipos de crimes cibernéticos que desafiam a aplicação do direito tradicional. Este trabalho visa analisar os principais aspectos relacionados aos crimes cibernéticos, abordando suas diversas formas e os métodos de combate adotados pelos sistemas jurídicos.

Palavras-chave: Crimes cibernéticos, Legislação, Investigação forense, Segurança da informação, Prevenção

Abstract/Resumen/Résumé

Globalization and technological evolution have transformed the way information is shared and protected. With the increasing use of the internet, new types of cyber crimes emerge, challenging the application of traditional law. This paper aims to analyze the main aspects related to cyber crimes, addressing their various forms and the combat methods adopted by legal systems.

Keywords/Palabras-claves/Mots-clés: Cyber crimes, Legislation, Forensic investigation, Information security, Prevention

1 Introdução

A globalização e a evolução tecnológica transformaram a forma como a informação é compartilhada e protegida. Com o uso da internet, surgem novos tipos de crimes cibernéticos que desafiam a aplicação do direito tradicional, pois ela revolucionou o comportamento humano, trouxe inúmeros benefícios a usuários e empresas, possibilitando a comunicação em tempo real e a troca de informações de maneira eficiente e rápida, mas trouxe vulnerabilidades, criando uma modalidade de crimes, como fraude, roubo de identidade, espionagem e ataques cibernéticos, que se tornaram comuns e exigiram uma reavaliação das leis e práticas de segurança, requerendo uma abordagem específica de prevenção e combate.

Este trabalho objetiva analisar os principais aspectos relacionados aos crimes cibernéticos, abordando suas diversas formas e os métodos de combate adotados pelos sistemas jurídicos. As fontes incluem livros especializados, artigos científicos e relatórios de organismos internacionais. A pesquisa é dividida em três etapas principais: levantamento teórico, análise das práticas de combate aos crimes cibernéticos e avaliação das políticas de segurança da informação.

2 Desenvolvimento

O objetivo geral é analisar a evolução dos crimes cibernéticos e as estratégias jurídicas e técnicas utilizadas para seu combate. Os objetivos específicos são investigar as principais tipologias de crimes cibernéticos e suas características; examinar a adequação das legislações vigentes no combate a esses crimes; analisar os métodos de investigação e prevenção adotados pela polícia e pelo judiciário; avaliar a eficácia das medidas preventivas e repressivas no contexto brasileiro e internacional. Este estudo utiliza uma abordagem qualitativa com revisão bibliográfica e análise documental dos principais textos legais, doutrinas e jurisprudências sobre crimes cibernéticos.

Os crimes cibernéticos podem ser classificados em próprios, impróprios e mistos. Entre os crimes próprios, destacam-se as fraudes bancárias eletrônicas, phishing, pharming e a distribuição de malwares, que possuem características únicas que dificultam sua investigação e punição, exigindo métodos específicos de análise de dados e rastreamento digital. As Fraudes Bancárias Eletrônicas envolvem o uso de informações bancárias obtidas ilegalmente

para realizar transações fraudulentas. Este tipo de crime explora vulnerabilidades nos sistemas de segurança de bancos e dos próprios usuários e podem ocorrer por meio da instalação de malwares que capturam informações bancárias, por meio de técnicas de engenharia social que induzem as vítimas a fornecerem seus dados ou pela exploração de falhas nos sistemas de *internet banking*. Segundo Santos (2009), "as fraudes bancárias eletrônicas são caracterizadas pelo uso indevido de dados financeiros obtidos por meio de técnicas de engenharia social ou de malwares instalados nos dispositivos das vítimas" .

Phishing e *Pharming* são técnicas de engenharia social que induzem os usuários a fornecerem informações confidenciais, como senhas e dados bancários. Os criminosos utilizam e-mails falsos e sites clonados para enganar as vítimas. O *phishing* envolve o envio de mensagens que parecem legítimas, mas que redirecionam os usuários para sites falsos, onde suas informações são roubadas. Já o *pharming* redireciona automaticamente o tráfego de internet para sites falsos, mesmo quando a URL correta é digitada. Conforme Cassanti (2014), "o phishing é uma técnica que se aproveita da ingenuidade dos usuários, para obter informações sensíveis, utilizando e-mails e sites fraudulentos que se passam por entidades confiáveis" .

Malwares incluem vírus, *trojans*, *worms* e *ransomwares*. Esses programas maliciosos podem danificar sistemas, roubar informações ou extorquir dinheiro das vítimas. A engenharia social é frequentemente usada para espalhar esses programas. Os *malwares* podem se instalar por meio de *downloads*, *e-mails* ou visitas a sites comprometidos, e uma vez instalados, podem realizar uma variedade de ações maliciosas, como roubo de dados, espionagem e destruição de arquivos. Conforme os organizadores Bezerra e Agnoletto (2020), "os *malwares* são programas desenvolvidos com o intuito de causar danos, ou obter acesso não autorizado a sistemas de computadores, muitas vezes distribuídos por meio de anexos de *e-mail*, ou *downloads* aparentemente inofensivos" .

Cavalos de Troia (*Trojans*) são programas que parecem legítimos, mas contém código malicioso que pode criar *backdoors*, permitindo que criminosos acessem o sistema da vítima remotamente. *Trojans* são frequentemente utilizados para instalar *keyloggers*, programas que registram todas as teclas digitadas pela vítima, capturando assim senhas e outras informações sensíveis. Conforme Barreto e Silveira (2016), "os Cavalos de Troia representam uma séria ameaça à segurança digital, pois permitem o controle remoto de

sistemas comprometidos, muitas vezes sem o conhecimento do usuário" .

Ransomwares são programas que bloqueiam o acesso ao sistema da vítima, ou criptografam seus dados, exigindo um pagamento, ou resgate, para liberar o acesso. Esse tipo de ataque tem se tornado cada vez mais comum, afetando tanto indivíduos quanto grandes organizações. A melhor defesa contra *ransomwares* é a prevenção, incluindo a realização de *backups* regulares e a utilização de *softwares* de segurança atualizados.

A legislação brasileira, incluindo a Lei nº 12.737/2012 (Lei Carolina Dieckmann), ainda é incipiente e apresenta lacunas na prevenção e repressão dos crimes cibernéticos. Esta lei, que surgiu após o vazamento de fotos íntimas da atriz Carolina Dieckmann, tipificou os crimes cibernéticos no Brasil, mas não abrange todas as nuances das atividades ilícitas *online*.

O Marco Civil da Internet estabelece direitos e deveres para usuários e provedores de internet no Brasil, mas precisa de complementação, para enfrentar a complexidade dos crimes cibernéticos. A proteção de dados pessoais e a privacidade dos usuários são temas centrais desta legislação, mas a implementação e fiscalização ainda são desafiadoras. O Marco Civil foi um avanço importante na regulamentação do uso da internet no Brasil, mas ainda existem muitas áreas que precisam ser aprimoradas, para oferecer uma proteção mais eficaz contra crimes cibernéticos. A Lei Geral de Proteção de Dados (LGPD) entrou em vigor em 2020 e visa proteger os dados pessoais dos cidadãos. A LGPD impõe responsabilidades, tanto para empresas, quanto para órgãos públicos no tratamento e proteção desses dados, contribuindo para a segurança digital e a prevenção de crimes cibernéticos. Ela estabelece direitos dos titulares dos dados, como o direito de acesso, correção e exclusão de suas informações pessoais. A implementação da LGPD representa um passo importante na adaptação do Brasil às normas internacionais de proteção de dados, como o GDPR na União Europeia. Segundo Barreto e Silveira (2016), "a LGPD é fundamental para garantir a privacidade e a segurança dos dados pessoais, criando um ambiente mais seguro às transações digitais e prevenindo abusos e crimes cibernéticos" .

Embora existam leis específicas para combater crimes cibernéticos, a rápida evolução da tecnologia e das técnicas utilizadas pelos criminosos supera a capacidade de resposta das legislações vigentes. A complexidade dos crimes cibernéticos exige uma atualização constante das leis e uma maior cooperação internacional, para lidar com atividades criminosas que frequentemente cruzam fronteiras. A Polícia Federal e outras

agências utilizam técnicas avançadas de análise forense computacional, incluindo a coleta e preservação de evidências digitais, o uso de softwares, para análise de sistemas, e a quebra de sigilo de dados. A investigação de crimes cibernéticos requer uma abordagem multidisciplinar, envolvendo conhecimentos em tecnologia da informação, direito e criminologia.

O Projeto Tentáculos exemplifica uma abordagem inovadora na investigação de fraudes bancárias cibernéticas, mostrando a importância da cooperação internacional e do uso de tecnologias de ponta. Este projeto envolve a colaboração entre diversas instituições, tanto nacionais quanto internacionais, para rastrear e combater atividades criminosas *online*. A troca de informações e a utilização de bancos de dados compartilhados são fundamentais para a eficácia dessas investigações.

Técnicas Forenses Digitais incluem a análise de discos rígidos, recuperação de dados deletados, monitoramento de atividades online e rastreamento de endereços IP. A perícia digital é essencial, para a identificação e preservação de evidências que possam ser utilizadas em processos judiciais. Ferramentas avançadas de *software* permitem a análise de grandes volumes de dados e a identificação de padrões que podem indicar atividades criminosas. De acordo com Santos (2009), "a perícia digital é um campo essencial na investigação de crimes cibernéticos, permitindo a coleta e análise de evidências digitais, que são cruciais para a elucidação de casos" . Desafios na investigação são a anonimidade proporcionada pela internet e o uso de tecnologias como criptografia e redes de anonimato (como a Tor), que dificultam a identificação dos criminosos. Além disso, a jurisdição limitada e a necessidade de cooperação internacional, muitas vezes, atrasam, ou complicam, as investigações. A formação e capacitação contínua de profissionais são importantes, para acompanhar as inovações tecnológicas e aprimorar as técnicas de investigação. O Manual de Investigação Cibernética à luz do Marco Civil da Internet, aborda técnicas específicas de preservação de evidências digitais, como a solicitação de registros de conexão e de aplicações de internet, o uso de ferramentas de análise forense e a importância da cooperação internacional. O manual, inclusive, discute a importância de procedimentos padronizados, para a coleta e preservação de provas digitais, garantindo a integridade e a admissibilidade dessas provas em processos judiciais .

A prevenção de crimes cibernéticos depende da conscientização dos usuários e da

adoção de boas práticas de segurança digital. A educação digital é fundamental, para que os usuários saibam identificar e evitar ameaças online. Medidas preventivas incluem o uso de antivírus, *firewalls*, senhas fortes e a atualização constante de *softwares*. Além disso, campanhas de conscientização sobre segurança digital são essenciais, para informar a população sobre os riscos e as formas de se proteger. A implementação de políticas de segurança da informação nas empresas e instituições públicas é crucial, para reduzir a vulnerabilidade a ataques cibernéticos.

Repressão efetiva requer uma infraestrutura legal robusta e uma capacitação contínua dos profissionais do direito e da segurança da informação. A atuação conjunta de órgãos de segurança, empresas de tecnologia e a cooperação internacional são essenciais, para combater eficazmente os crimes cibernéticos. A criação de unidades especializadas em crimes cibernéticos dentro das forças de segurança e a promoção de parcerias com o setor privado são estratégias importantes para aprimorar a resposta a essas ameaças.

Desafios na prevenção estão na rápida evolução das técnicas de ataque e a falta de conhecimento técnico de muitos usuários, o que tornam a prevenção um desafio contínuo. A educação e a conscientização são fundamentais, mas precisam ser acompanhadas por uma infraestrutura de segurança robusta e atualizada. A inclusão de temas relacionados à segurança digital nos currículos escolares e a promoção de treinamentos, para profissionais de diversas áreas, são medidas que podem contribuir significativamente para a prevenção de crimes cibernéticos.

A tipicidade penal em crimes cibernéticos envolve a necessidade de definir claramente as condutas que constituem crimes no ambiente digital. Segundo Brito (2013), "a tipicidade é a adequação perfeita da conduta do agente ao tipo penal descrito na lei. No ciberespaço, essa definição se torna ainda mais complexa devido à natureza dinâmica e inovadora das tecnologias". A falta de clareza na legislação pode resultar em dificuldades para a aplicação da lei e a punição dos infratores.Nos crimes cibernéticos, o sujeito ativo é o agente que pratica a conduta criminosa, enquanto o sujeito passivo é a vítima que sofre a lesão, ou ameaça de lesão, a um bem jurídico protegido. Conforme Brito (2013), "os crimes cibernéticos podem ser praticados por indivíduos ou grupos organizados, muitas vezes anônimos ou utilizando identidades falsas. As vítimas podem ser pessoas físicas, jurídicas ou até mesmo o Estado". A identificação dos sujeitos ativos é um dos maiores desafios às

autoridades.

A aplicação da lei penal no ciberespaço enfrenta desafios específicos devido à natureza transnacional da internet. Brito (2013) afirma que "a internet não respeita fronteiras geográficas, o que complica a aplicação das leis nacionais. A cooperação internacional e a harmonização das legislações são essenciais para enfrentar essa questão". A extraterritorialidade e a necessidade de acordos bilaterais ou multilaterais são temas recorrentes nas discussões sobre jurisdição em crimes cibernéticos.

A fixação de competência para julgar crimes cibernéticos envolve a determinação do foro adequado para processar e julgar os delitos. De acordo com Brito (2013), "a competência pode ser estabelecida com base no local onde ocorreu o resultado do crime, onde se encontra o agente, ou onde a conduta foi praticada. No caso de crimes cibernéticos, essa definição é particularmente desafiadora devido à ubiquidade da internet". A definição clara de competência é essencial para garantir a eficácia do processo penal e a aplicação justa da lei.

3 Conclusão

Os crimes cibernéticos são desafios significativos para o sistema jurídico e para as autoridades de segurança, pois a evolução rápida da tecnologia exige uma constante adaptação das leis e dos métodos de investigação. É essencial que os Estados promovam a cooperação internacional e invistam em tecnologias e treinamentos, para garantir a proteção eficaz contra essas novas formas de criminalidade. O aprimoramento das legislações, aliado à educação digital e à colaboração entre as nações, é crucial para a construção de um ambiente digital mais seguro e confiável. A importância da cooperação internacional não pode ser subestimada, pois muitos crimes cibernéticos são transnacionais por natureza. A colaboração entre diferentes países, por meio de tratados e acordos de assistência mútua, é fundamental para a identificação, captura e julgamento de criminosos cibernéticos, bem como a troca de informações e a adoção de padrões comuns de segurança, que podem ajudar a fortalecer a capacidade global de resposta a essas ameaças.

4 Referências

BARRETO, Alesandro Gonçalves; BRASIL, Beatriz Silveira. *Manual de Investigação Cibernética À luz do Marco Civil da Internet*. São Paulo; Brasport, 2016.

BEZERRA, Clayton da Silva; AGNOLETTO, Giovani Celso *Combate ao Crime Cibernético - Doutrina e Prática – A visão do delegado de polícia.* 1.ed.Rio de Janeiro; Mallet Editora, 2020.

BRITO, Auriney. *Direito Penal Informático*. São Paulo; Editora Saraiva, 2013

CASSANTI, Moisés de Oliveira. *Crimes Virtuais, Vítimas Reais*. São Paulo; Brasport, 2014.

DENG, Xinhao; LI, Qi; XU, Ke. Robust and reliable early-stage website fingerprinting attacks via spatial-temporal distribution analysis. In: Proceedings of the 2024 ACM

SÁ, Alan Oliveira de; **PRADO,** Charles Bezerra; **FLÁVIO**, Mariana Luiza; **CARMO**, Luiz F. Rust da C. Intelligent attacks on cyber-physical systems and critical infrastructures. In: DAPONTE, Pasquale; KŁOSAK, Maciej; BENDARMA, Amine (Ed.). Modern technologies enabling innovative methods for maritime monitoring and strengthening resilience in maritime critical infrastructures. NATO Science for Peace and Security Series - D: Information and Communication Security, v. 65, p. 332–351, 2024. DOI: https://doi.org/10.3233/NICSP240033.

SANTOS, Coriolano Aurélio de Almeida Camargo. *As múltiplas faces dos crimes eletrônicos e dos fenômenos tecnológicos e seus reflexos no universo jurídico*. São Paulo; OAB SP, 2009.

SIGSAC Conference on Computer and Communications Security (CCS '24), Salt Lake City, UT, USA, 14–18 out. 2024. New York: ACM, 2024. DOI: https://doi.org/10.1145/3658644.3670272.