

**II CONGRESSO INTERNACIONAL DE
DIREITO, POLÍTICAS PÚBLICAS,
TECNOLOGIA E INTERNET**

DIREITO PENAL E CIBERCRIMES

D598

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

Coordenadores: Ana Carolina de Sá Juzo, Lucas Gonçalves da Silva e Helen Cristina de Almeida Silva – Franca: Faculdade de Direito de Franca, 2024.

Inclui bibliografia

ISBN: 978-65-5274-015-1

Modo de acesso: www.conpedi.org.br em publicações

Tema: Regulação do Ciberespaço.

1. Ciber Crimes. 2. Fraudes Virtuais. 3. Deep Web. 4. Políticas Públicas de Desenvolvimento. 5. Efetividade do Direito. I. II Congresso Internacional de Direito, Políticas Públicas, Tecnologia e Internet (1:2024 : Franca, SP).

CDU: 34

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

DIREITO PENAL E CIBERCRIMES

Apresentação

Entre os dias 27 e 30 de agosto de 2024, a Faculdade de Direito de Franca recebeu o 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 – Direito Penal e Cibercrimes tratou dos desafios do direito penal no contexto dos cibercrimes, destacando as transformações tecnológicas e os novos tipos de crimes virtuais que demandam respostas inovadoras do sistema jurídico. As discussões exploraram as tecnologias aplicadas à investigação criminal e os desafios jurisdicionais associados a crimes eletrônicos, incluindo fraudes virtuais, ataques realizados por hackers e crackers, e os riscos associados à Deep Web e à Dark Web. O uso das redes sociais como meio para atividades criminosas e a aplicação de reconhecimento facial na persecução penal também foram amplamente debatidos, evidenciando a necessidade de regulamentações específicas e de ferramentas tecnológicas para a segurança e a justiça no ambiente digital.

**CIBERSEGURANÇA E DIREITO PENAL: ANÁLISE DA APLICAÇÃO DA LEI
12.737/2012 - LEI CAROLINA DIECKMANN**

**CYBERSECURITY AND CRIMINAL LAW: ANALYSIS OF THE APPLICATION
OF LAW 12.737/2012 - CAROLINA DIECKMANN LAW**

**Maria Eduarda de Oliveira Silva
Vinicius De Sousa Damasceno**

Resumo

O tema da pesquisa é a aplicação Lei 12.737/2012 (Lei Carolina Dieckmann) no contexto da cibersegurança no Brasil. A pesquisa tem como objetivo geral analisar a proteção oferecida pela lei aos indivíduos no ambiente digital, com objetivos específicos de entender a evolução dos crimes cibernéticos, avaliar a eficácia da lei na proteção de dados pessoais e na prevenção de violações de privacidade, e analisar os desafios impostos pelas constantes mudanças tecnológicas. A metodologia adotada inclui abordagem dialética, pesquisa bibliográfica e abordagem qualitativa para investigar e compreender as complexidades da aplicação prática da legislação.

Palavras-chave: Cibersegurança, Lei carolina dieckmann, Crimes cibernéticos

Abstract/Resumen/Résumé

The research topic is the effectiveness of Law 12.737/2012 (Carolina Dieckmann Law) in the context of cybersecurity in Brazil. The general objective of the research is to analyze the protection offered by the law to individuals in the digital environment. The specific objectives include understanding the evolution of cybercrimes, evaluating the effectiveness of the law in protecting personal data and preventing privacy violations, and analyzing the challenges posed by constant technological changes. The methodology adopted includes a dialectical approach, bibliographic research, and a qualitative approach to investigate and understand the complexities of the practical application of the legislation.

Keywords/Palabras-claves/Mots-clés: Cybersecurity, Carolina dieckmann law, Cybercrimes

1 INTRODUÇÃO

A cibersegurança tornou-se um tema de extrema relevância na era digital, onde a interconectividade e a dependência de sistemas informáticos são cada vez mais presentes em todos os aspectos da vida moderna. Com o aumento das ameaças cibernéticas, como ataques de hackers, roubo de dados pessoais e fraudes online, surge a necessidade de legislações que protejam a integridade e a privacidade dos indivíduos e organizações. No contexto brasileiro, a Lei nº 12.737/2012, popularmente conhecida como Lei Carolina Dieckmann, é uma resposta significativa a essas ameaças. Nomeada em referência à atriz brasileira que teve fotos pessoais expostas na internet sem consentimento, esta lei alterou o Código Penal Brasileiro para tipificar crimes informáticos específicos.

Portanto, a pesquisa questiona, é eficaz a aplicação da Lei 12.737/2012 (Lei Carolina Dieckmann) quanto à proteção da privacidade e da segurança cibernética? Para que uma lei seja eficaz, é fundamental que sua redação seja clara e precisa, evitando ambiguidades que possam gerar diferentes interpretações e dificultar sua aplicação. Além disso, a lei deve ser adequada à realidade social, econômica e tecnológica do contexto em que será aplicada, refletindo as necessidades e os desafios contemporâneos.

A capacitação dos profissionais responsáveis por sua implementação, como juízes, promotores e policiais, é essencial para garantir que a lei seja aplicada corretamente e de maneira justa, bem como a infraestrutura adequada e os recursos necessários também são críticos, pois permitem a execução das ações previstas pela lei. Além disso, é importante que haja uma conscientização e educação da população sobre os direitos e deveres estabelecidos, garantindo o cumprimento voluntário e a aceitação social da norma.

O objetivo geral é analisar essa interação no contexto da cibersegurança, visando compreender como essa legislação protege os indivíduos no ambiente digital. Os objetivos específicos deste estudo são: compreender a evolução dos crimes cibernéticos e a importância de uma tipificação adequada para assegurar penas proporcionais; avaliar a eficácia da Lei Carolina Dieckmann na proteção de dados pessoais e na prevenção de violações de privacidade; e analisar o desafio da constante mudança no espaço digital que implica na aplicação da legislação.

Para a celebração do presente trabalho, foi utilizado a abordagem dialética foi empregada como método científico, permitindo a investigação crítica e a compreensão das contradições e relações entre diferentes aspectos da legislação e sua aplicação prática. O método exploratório orientou o estudo ao investigar novas perspectivas e possibilitar a descoberta de

questões anteriormente não considerados, fundamentais para entender a complexidade do tema. A pesquisa bibliográfica foi essencial como procedimento técnico, fornecendo uma base sólida de conhecimento através da revisão de literatura existente, incluindo artigos acadêmicos, textos legais e relatórios especializados. Por fim, foi adotado também a abordagem qualitativa, pois Segundo Triviños, “a abordagem de cunho qualitativo trabalha os dados buscando seu significado, tendo como base a percepção do fenômeno dentro do seu contexto”. (TRIVIÑOS, 1987, *apud.* OLIVEIRA, 2011, p. 25).

2 EVOLUÇÃO DOS CRIMES CIBERNÉTICOS E A NECESSIDADE DE TIPIFICAÇÃO ADEQUADA

A lei 12.737/2012 trouxe os primeiros casos significativos de crimes cibernéticos no Brasil. Os crimes foram classificados em grupos criminosos gerais sem qualquer legislação específica, que muitas vezes não eram adequados à complexidade do comportamento online. Invasão de privacidade, roubo de dados, fraude na internet, roubo, apropriação indébita, etc. Eram disposições criminais tradicionais utilizadas para tratar casos de invasão de privacidade, roubo de dados, etc.

O conceito de proteção de dados centra-se na salvaguarda da personalidade do indivíduo, e não nos seus bens. É um direito pessoal e de segurança que é parte integrante da experiência humana, pois é uma expressão tangível da liberdade e da dignidade de um indivíduo (FREITAS, 2020).

Com a popularização da internet e a crescente digitalização das atividades econômicas e sociais, houve um aumento exponencial na incidência de crimes cibernéticos. A falta de tipificações específicas gerava insegurança jurídica e dificuldades na aplicação de penas proporcionais às novas modalidades de condutas ilícitas.

Como não havia lei sobre crimes cibernéticos, existia muitas inconsistências e divergências ao se tratar desse assunto. Hackeava-se muitos dispositivos informáticos, onde se espalhava vírus e, até mesmo, acabavam interceptando comunicações eletrônicas. O código penal não previa disposições suficientes para resolver essas questões, acarretando às dificuldades em processar e punir os infratores.

De acordo com o artigo 154-A do código penal, advindo da Lei Carolina Dieckmann, a tipificação do acesso não autorizado a equipamentos de informática tornou-se mais clara e objetiva, permitindo que os criminosos respondessem de forma mais adequada e proporcional aos crimes emergentes, melhorando a capacidade do sistema jurídico de lidar com as especificidades dos crimes digitais.

3 EFICÁCIA DA LEI 12.737/2012 E A CONSTANTE MUDANÇA NO ESPAÇO DIGITAL

A eficácia da Lei 12.737/2012 enfrenta desafios significativos devido à natureza dinâmica e em constante evolução do espaço digital. Quando a lei foi promulgada, ela trouxe inovações importantes ao tipificar crimes cibernéticos e ao buscar proteger a privacidade dos indivíduos. No entanto, a rápida evolução da tecnologia e das ameaças cibernéticas coloca à prova a capacidade dessa legislação de permanecer eficaz e relevante.

Uma das maiores dificuldades na regulamentação do espaço digital é a velocidade com que novas tecnologias e ameaças surgem. A internet e os dispositivos conectados estão em constante transformação, com novas formas de comunicação, armazenamento de dados e interações online sendo desenvolvidas continuamente. Isso resulta em um cenário onde as ameaças cibernéticas também evoluem rapidamente, com criminosos cibernéticos encontrando constantemente novas maneiras de explorar vulnerabilidades e cometer crimes.

A Lei Carolina Dieckmann, embora tenha sido um passo significativo à época de sua criação, precisa ser periodicamente revisada e atualizada para lidar com essas novas formas de ameaças, como o ransomware, ataques de engenharia social mais sofisticados, e o uso indevido de tecnologias emergentes como a inteligência artificial.

Diante de tantas lacunas, a lei apesar da sua importância, não consegue amparar boa parte da sociedade, pois umas parcelas de indivíduos são legais em relação a de segurança ou até mesmo não possuem recursos suficientes para arcar com a instalação de programas, como antivírus ou quaisquer outros que sirvam como forma de proteção pessoal dos seus dados. (SÁ, 2021,p. 11)

A adaptação das leis ao ritmo das mudanças tecnológicas não é uma tarefa fácil. O processo legislativo é geralmente mais lento e burocrático do que o ritmo das inovações

tecnológicas. Isso cria um descompasso entre a realidade das ameaças cibernéticas e a capacidade das leis de combatê-las eficazmente. Além disso, a falta de uma terminologia padronizada e a complexidade técnica das novas ameaças dificultam a redação de leis que sejam abrangentes e precisas ao mesmo tempo.

4 CONCLUSÃO

A interação entre a Lei 12.737/2012, conhecida como Lei Carolina Dieckmann, e o Direito Penal no contexto da cibersegurança é fundamental para a proteção da privacidade e segurança dos indivíduos no ambiente digital. A legislação trouxe avanços significativos na tipificação de crimes cibernéticos, porém enfrenta desafios na sua aplicação prática devido à constante evolução tecnológica. Essa dinâmica exige adaptações legislativas contínuas e investimentos em capacitação e tecnologia. Com as devidas melhorias e a colaboração entre diferentes setores, é possível fortalecer a proteção dos cidadãos no ambiente virtual, garantindo um espaço digital mais seguro e respeitoso à privacidade.

REFERÊNCIAS

DEFENSORIA PÚBLICA DO ESTADO DO CEARÁ. Lei Carolina Dieckmann: 10 anos da lei que protege a privacidade dos brasileiros no ambiente virtual. Disponível em: <<https://www.defensoria.ce.def.br/noticia/lei-carolina-dieckmann-10-anos-da-lei-que-protege-a-privacidade-dos-brasileiros-no-ambiente-virtual/>>. Acesso em: 18 abr. 2024.

BARRETO, Erick Teixeira. Crimes cibernéticos sob a égide da Lei n. 12.737/2012, março 2017. Disponível em: <<http://www.conteudojuridico.com.br/consulta/artigos/49678/crimes-ciberneticos-sobaegide-da-lei-12-737-2012>>. Acesso em: 18 abr. 2024.

FREITAS, C. C. G. de; GONÇALVES, J. R.; TORRES, M. G. A evolução do direito penal brasileiro relacionado aos crimes cibernéticos. Revista JRG de Estudos Acadêmicos, Brasil, São Paulo, v. 6, n. 12, p. 296–311, 2023. DOI: 10.5281/zenodo.7760710. Disponível em: <<http://www.revistajrg.com/index.php/jrg/article/view/520>>. Acesso em: 13 jun. 2024.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/112737.htm>. Acesso em: 20 abr. 2024.