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

DIREITO PENAL E CIBERCRIMES I

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

Coordenadores: Clóvis Alberto Volpe Filho, Helen Cristina de Almeida e Lucas Gonçalves da Silva – Franca: Faculdade de Direito de Franca, 2025.

Inclui bibliografia
ISBN: 978-65-5274-370-1
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 I

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 examina as novas fronteiras do direito penal em meio à criminalidade virtual. As comunicações abordam o uso de reconhecimento facial, deepfakes e provas digitais, destacando riscos à privacidade e à integridade processual. O grupo busca construir parâmetros jurídicos que assegurem a proteção de direitos fundamentais diante dos desafios tecnológicos contemporâneos.

DARK WEB E CYBER CRIMES

DARK WEB AND CYBER CRIMES

Manuela Demacq Chierintin
Lara De Russi Rocha
Luiz Felipe Cardoso

Resumo

O presente trabalho analisa a relação entre a Dark Web e os crimes cibernéticos, destacando como o anonimato e a criptografia favorecem a prática de atividades ilícitas no ambiente virtual. Abordam-se as principais dificuldades enfrentadas pelas autoridades brasileiras na investigação desses crimes, tanto do ponto de vista técnico quanto jurídico. A ausência de legislação específica, a necessidade de cooperação internacional e a defasagem na capacitação dos operadores do Direito são apontadas como entraves ao enfrentamento eficaz do problema. Conclui-se que a repressão a esses crimes exige atualização normativa, integração global e investimento em inteligência cibernética.

Palavras-chave: Dark web, Crimes cibernéticos, Investigação digital, Direito penal, Cooperação internacional

Abstract/Resumen/Résumé

This paper analyzes the relationship between the Dark Web and cybercrimes, emphasizing how anonymity and encryption foster illegal activities in the virtual environment. It examines the main challenges faced by Brazilian authorities in investigating these crimes, both from technical and legal perspectives. The lack of specific legislation, the need for international cooperation, and the gap in training for legal professionals are identified as major obstacles to effective enforcement. The study concludes that repressing such crimes requires legal modernization, global integration, and investment in cyber intelligence.

Keywords/Palabras-claves/Mots-clés: Dark web, Cybercrime, Digital investigation, Criminal law, International cooperation

DARK WEB E CYBER CRIMES

Uma análise das práticas criminosas no submundo digital contemporâneo

1 INTRODUÇÃO

Com o avanço da tecnologia e a globalização, surgem também novas formas de criminalidade, especialmente no ambiente virtual. A Dark Web, uma camada oculta da internet, destaca-se como um espaço onde o anonimato e a criptografia favorecem a prática de diversos crimes cibernéticos. O presente resumo expandido tem como objetivo analisar o papel da Dark Web na propagação dessas atividades ilícitas, discutindo seus impactos, os desafios enfrentados pelas autoridades e os obstáculos jurídicos que dificultam sua repressão eficaz.

O desenvolvimento constante da internet trouxe diversas facilidades em âmbito global, permitindo a conexão mais simples em grandes distâncias. Entretanto, essa evolução trouxe com ela a ampliação do risco à intimidade, privacidade e à segurança dos usuários. Com certeza, os avanços tecnológicos ainda proporcionam vantagens à sociedade em geral, porém também incentivam a proliferação de crimes – sendo a Dark Web um exemplo emblemático, por abrigar conteúdos e atos ilícitos difíceis de identificar e combater.

Diferenciando-se da rede comum, utilizada pela grande maioria da população, a Dark Web não pode ser acessada por todos. Seu uso exige navegadores específicos e oferece como principais características o anonimato dos usuários e a grande dificuldade de rastreá-los. As transações dos produtos vendidos são frequentemente realizadas por meio de criptomoedas, como o Bitcoin, o que dificulta ainda mais o rastreamento tanto dos vendedores quanto dos compradores. Essa combinação de fatores torna a Dark Web um ambiente propício para a disseminação de atividades criminosas, desafiando as autoridades responsáveis pela segurança digital.

No Brasil, a prática de crimes cibernéticos tem se tornado cada vez mais frequente. Devido às características da Dark Web e à ausência de legislação eficiente e capaz de combatê-la, têm-se tornado mais acessíveis a realização e propagação de atos criminosos cibernéticos. Tendo em vista a necessidade de repressão a esses criminosos, é

preciso estudar os desafios jurídicos na coibição e investigação dos crimes virtuais, objetivando maior segurança e privacidade do usuário. Portanto, é primordial investigar os empecilhos na aplicação do Direito de maneira concreta no ambiente virtual. Então, de que maneira a Dark Web está contribuindo para os crimes cibernéticos?

A metodologia adotada é de caráter dedutivo, com enfoque em pesquisa qualitativa e exploratória, por meio de análise bibliográfica e documental.

2 DESENVOLVIMENTO

A expansão do ciberespaço proporcionou a criação de ambientes virtuais em que práticas criminosas se tornaram mais sofisticadas, sobretudo no âmbito da Dark Web. Este segmento da internet profunda caracteriza-se por seu acesso restrito, por meio de softwares específicos como o Tor, que permitem a navegação anônima e a ocultação de endereços IP, dificultando sobremaneira a identificação de usuários e administradores de páginas ilegais. Tais características têm favorecido a disseminação de mercados ilícitos, comércio de substâncias proibidas, exploração sexual infantil, tráfico de armas e venda de dados pessoais, atividades que desafiam permanentemente os sistemas jurídicos e investigativos em âmbito nacional e internacional.

No Brasil, a investigação de crimes cometidos na Dark Web encontra barreiras tanto de natureza técnica quanto jurídica. Em termos técnicos, os mecanismos de anonimização e criptografia empregados na Deep e na Dark Web inviabilizam, na maioria das vezes, a coleta convencional de provas digitais. Para a Polícia Judiciária, muitas vezes torna-se necessário recorrer a cooperações internacionais, compartilhamento de dados com empresas privadas e uso de técnicas avançadas de rastreamento digital, como análise de blockchain, monitoramento de transações financeiras e infiltração de agentes virtuais em fóruns criminosos.

Sob o prisma jurídico, destaca-se a dificuldade de compatibilizar o respeito às garantias constitucionais do devido processo legal, do contraditório e da ampla defesa com a necessidade de investigação eficaz. O anonimato garantido por tecnologias de criptografia robusta frequentemente conduz à produção de provas que dependem de medidas excepcionais, como a quebra de sigilo telemático e a interceptação de comunicações eletrônicas, as quais exigem autorização judicial fundamentada.

Ademais, a própria legislação brasileira ainda carece de dispositivos específicos que abarquem todas as nuances do crime cibernético praticado na Dark Web, sendo comum a aplicação subsidiária do Código Penal e do Marco Civil da Internet (Lei nº 12.965/2014), que, embora relevantes, não contemplam de maneira abrangente as singularidades desse ambiente.

Outro desafio relevante diz respeito à cooperação internacional. A natureza transnacional dos delitos virtuais exige integração com órgãos estrangeiros e organismos de segurança, como a Interpol e Europol, além dos tratados e convenções internacionais, como a Convenção de Budapeste, que o Brasil ainda não ratificou.

Por fim, observa-se que a própria formação técnica de operadores do Direito e agentes de segurança pública, em muitos casos, não acompanha a velocidade da evolução tecnológica. A necessidade de capacitação, somada ao investimento em infraestrutura digital e inteligência cibernética, torna-se condição essencial para o enfrentamento eficaz dos crimes na Dark Web. É evidente que os desafios jurídicos e operacionais são múltiplos e exigem uma abordagem que envolva uma modernização legislativa, cooperação internacional e novas técnicas investigativas que sejam efetivas dentro deste ambiente obscuro.

3 CONCLUSÃO

A análise dos crimes cibernéticos vinculados à Dark Web evidencia a complexidade do fenômeno e os desafios para enfrentá-lo. A combinação de anonimato, descentralização e sofisticação tecnológica torna a Dark Web um ambiente propício para práticas ilícitas que transcendem fronteiras geográficas e jurisdicionais.

Embora medidas como tratados internacionais, investimentos em tecnologia forense e ações coordenadas entre governos venham sendo implementadas, é notável que a prevenção e o combate eficaz ao crime cibernético na Dark Web exigem um esforço contínuo e multidisciplinar.

Além disso, é fundamental investir em educação digital e políticas públicas de conscientização, a fim de fortalecer a cultura da cibersegurança e reduzir a vulnerabilidade da população a práticas criminosas. Dessa forma, será possível avançar na construção de um ambiente digital mais seguro, ético e transparente.

Por fim, ressalta-se a importância do aprimoramento legislativo nacional, especialmente com a criação de normas específicas que abranjam as particularidades dos crimes praticados na Dark Web. A atualização constante do ordenamento jurídico, aliada ao uso estratégico de recursos tecnológicos pelas autoridades, pode proporcionar maior efetividade na responsabilização penal e na proteção dos direitos fundamentais dos usuários da internet.

4 REFERÊNCIAS

ALMEIDA, Thiago Pires; SOUSA, Larissa Gomes. A Profundidade da Deep Web: desafios legislativos e investigativos. Rio de Janeiro: Ed. Nova Lex, 2020.

ANDRADE, Jéssica de Souza. A Dark Web e os desafios à segurança cibernética. Revista de Direito, Estado e Internet, v. 6, n. 2, p. 45-60, 2022. Disponível em: https://revistas.unifacs.br/index.php/rdei/article/view/1435.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet. Diário Oficial da União, Brasília, DF, 24 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

CASTRO, Juliana Lopes. Criptoanálise e Cooperação Internacional no Combate aos Crimes Cibernéticos. Revista de Direito Penal e Criminologia, v. 8, n. 2, p. 119–140, 2021.

CONSELHO DA EUROPA. Convenção de Budapeste sobre o Crime Cibernético, 2001. Disponível em: https://www.coe.int/en/web/cybercrime/the-budapest-convention.

FERNANDES, Rafael. Crimes digitais e anonimato: um estudo sobre a atuação na Dark Web. Revista Brasileira de Criminologia, v. 4, n. 1, p. 99-115, 2021. Disponível em: https://revistabdc.direito.ufmg.br/index.php/revista/article/view/115.

MOURA, Camila Fernandes. Aspectos Processuais da Investigação Criminal na Dark Web. Revista Brasileira de Direito Digital, v. 12, n. 3, p. 45–72, 2019.

PAULINO, Larissa. Segurança cibernética no Brasil: desafios e perspectivas. São Paulo: Atlas, 2023.

PEREIRA, Bruno Santoro. Anonimato Digital: Limites e Potencialidades no Processo Penal Brasileiro. Porto Alegre: Editora Jurídica Nacional, 2017.

ROSA, Tiago. O papel das criptomoedas nos crimes da Dark Web. Revista de Economia Digital, v. 7, n. 3, p. 78-91, 2022. Disponível em: https://redigital.org.br/revista/article/view/72.