Cadeia de Custódia em Crimes Cibernéticos: Desafios, Tecnologias e Garantias Processuais

Autor(res)

Andressa Germann Avila
Daniel Germann Avila
Rhaylan Henrique Francisco De Souza

Categoria do Trabalho

Iniciação Científica

Instituição

PUC - PONTIFÍCIA UNIVERSIDADE CATÓLICA

Introdução

O avanço da tecnologia e a crescente digitalização da sociedade transformaram o panorama criminal, ampliando a incidência de crimes cibernéticos, como fraudes eletrônicas, invasões de sistemas e crimes contra a privacidade. A literatura aponta que a integridade das provas digitais é essencial para a efetividade do processo penal e para a segurança jurídica (Silva & Almeida, 2022; Ferreira, 2021). Diferentemente de provas físicas, evidências digitais são altamente suscetíveis à adulteração, perda ou contaminação, exigindo protocolos rigorosos de cadeia de custódia, documentação minuciosa e controle tecnológico. No contexto brasileiro, o Código de Processo Penal e legislações correlatas estabelecem diretrizes gerais sobre coleta de provas, mas a aplicação em crimes digitais apresenta desafios únicos, incluindo rastreabilidade de logs, autenticação de dados e preservação de metadados.

Objetivo

Analisar os desafios e estratégias da cadeia de custódia em crimes cibernéticos no Brasil, avaliando protocolos técnicos, tecnologias de rastreabilidade, capacitação de peritos, impacto na confiabilidade processual e contribuição para a segurança jurídica e efetividade do sistema penal.

Material e Métodos

A pesquisa utiliza abordagem qualitativa, exploratória e documental. Foram examinados processos judiciais envolvendo crimes cibernéticos entre 2015 e 2025, relatórios de perícia digital, legislações brasileiras aplicáveis e literatura científica sobre investigação digital, preservação de evidências e segurança processual. A análise de conteúdo permitiu identificar lacunas na prática forense, falhas na documentação, estratégias inovadoras de rastreabilidade e padrões internacionais de referência, como diretrizes da INTERPOL e FBI.

Resultados e Discussão

Os resultados indicam que a falta de padronização de protocolos e treinamento de peritos compromete a integridade das provas digitais e aumenta o risco de nulidades processuais. A integração de tecnologias como blockchain, criptografia avançada e sistemas de rastreamento digital mostrou-se eficaz na preservação de evidências e auditoria contínua (Silva, 2022; INTERPOL, 2021). A discussão evidencia que, para crimes

cibernéticos, a cadeia de custódia não é apenas procedimento técnico, mas instrumento crítico de segurança jurídica, confiabilidade judicial e prevenção de litígios, contribuindo significativamente para literatura acadêmica sobre direito penal digital. Contribuições inovadoras incluem protocolos híbridos de rastreabilidade, capacitação multidisciplinar de peritos e integração com inteligência artificial para detecção de adulterações e monitoramento contínuo.

Conclusão

A pesquisa conclui que a cadeia de custódia em crimes cibernéticos exige protocolos rigorosos, capacitação contínua de peritos e tecnologias avançadas de rastreabilidade. A implementação dessas estratégias garante integridade das provas, fortalece a segurança jurídica e contribui para confiabilidade processual. O estudo oferece contribuições inovadoras à literatura científica, ao propor integração tecnológica, auditoria contínua e métodos híbridos de preservação de evidências digitais.

Referências

Silva, R., & Almeida, P. (2022). Cadeia de Custódia e Perícia Digital. Revista Brasileira de Direito Penal e Tecnologias, 18(2), 45-78.
Ferreira, L. (2021). Crimes Cibernéticos e Segurança Processual. Journal of Digital Forensics, 14(1), 67-92.
INTERPOL. (2021). Guidelines on Digital Evidence Management. Lyon: INTERPOL.
FBI. (2020). Cybercrime Investigations and Evidence Integrity. Federal Bureau of Investigation.
Código de Processo Penal, Decreto-Lei nº 3.689/1941. Brasília: Diário Oficial da União.
Oliveira, M. (2021). Investigação Criminal Digital e Cadeia de Custódia. Revista de Estudos Penais, 17(3), 89-115.