CRIMES CIBERNÉTICOS -ESTELIONATO DIGITAL

Autor(res)

Regina Maria Pinna Trindade
Lucas Gonçales Thomaz
Patricia Lima
Anderson Akira Watanabe

Categoria do Trabalho

TCC

Instituição

FACULDADE ANHANGUERA DE GUARULHOS

Introdução

A revolução digital trouxe avanços significativos à sociedade contemporânea, transformando hábitos de consumo, comunicação e interação social. No entanto, esse desenvolvimento também abriu espaço para a prática de novas modalidades de crimes, conhecidos como crimes cibernéticos. Tais delitos se caracterizam pelo uso de dispositivos eletrônicos e redes digitais como instrumentos de fraude, extorsão, invasão de sistemas ou violação de dados pessoais. Entre as práticas mais recorrentes está o estelionato eletrônico, previsto no artigo 171, §2º do Código Penal, que consiste na obtenção de vantagem ilícita mediante engodo em ambiente virtual. A crescente sofisticação dessas práticas, como golpes via phishing, clonagem de aplicativos de mensagens e fraudes bancárias digitais, evidencia os desafios do Estado e do Direito Penal no enfrentamento dessa criminalidade. O tema ganha relevância não apenas pela gravidade dos prejuízos financeiros e sociais, mas também porque impacta direitos fundamentais como privacidade, segurança e confiança no ambiente digital. Nesse cenário, o estudo justifica-se pela necessidade de compreender os mecanismos jurídicos de combate ao estelionato virtual, identificar lacunas na legislação vigente e apontar caminhos que promovam uma regulação mais eficiente, equilibrando a repressão penal com a proteção de garantias individuais.

Objetivo

Investigar a evolução dos crimes cibernéticos no Brasil, com ênfase no estelionato eletrônico, analisando sua tipificação legal, desafios de investigação e julgamento, além de discutir o papel da legislação, da jurisprudência e da cooperação internacional no combate a tais delitos.

Material e Métodos

A pesquisa tem caráter bibliográfico e documental, fundamentada na análise de legislações nacionais (Constituição Federal, Código Penal, Código de Processo Penal, Lei 12.737/2012 – Lei Carolina Dieckmann, Lei 12.965/2014 – Marco Civil da Internet e Lei 13.709/2018 – LGPD), bem como tratados internacionais como a Convenção de Budapeste. Foram consultados livros de autores renomados, como Luiz Flávio Gomes, Rogério Greco, Cláudia Maria Barbosa e Damásio de Jesus, além de artigos científicos, relatórios de órgãos públicos, jurisprudências do STJ e manuais de investigação digital do Ministério Público Federal. O método consistiu na

sistematização de conceitos, classificação de crimes cibernéticos, estudo de casos emblemáticos e análise da legislação aplicável, buscando confrontar teoria e prática. Também foram consideradas estatísticas recentes de órgãos como FEBRABAN, Serasa Experian e Polícia Federal, que evidenciam o aumento expressivo das fraudes virtuais no Brasil.

Resultados e Discussão

Os resultados apontam que os crimes cibernéticos evoluíram de práticas pontuais, como a disseminação de vírus nos anos 1980, para fenômenos globais complexos, como ransomware, fraudes via Pix e golpes com deepfakes. O estelionato eletrônico destaca-se como uma das modalidades mais recorrentes e desafiadoras, dada a sua capacidade de se adaptar às novas tecnologias. Dados recentes da FEBRABAN e da Polícia Federal revelam que fraudes digitais cresceram mais de 30% em 2023, especialmente em transações bancárias e financeiras.

No campo jurídico, observa-se a ampliação da legislação, com destaque para a inclusão do §2º-A no art. 171 do Código Penal pela Lei 14.155/2021, que aumentou a pena para estelionato cometido por meio digital. A jurisprudência também tem evoluído: o STJ consolidou a responsabilidade objetiva dos bancos em casos de fraudes (Súmula 479), além de admitir a prisão preventiva de integrantes de organizações criminosas digitais. No entanto, persistem desafios como a definição de competência em crimes transnacionais, a lentidão investigativa e a dificuldade de obtenção de provas digitais válidas.

Além disso, a LGPD trouxe avanços importantes para a proteção de dados pessoais, impondo obrigações às empresas e criando a Autoridade Nacional de Proteção de Dados (ANPD). No entanto, casos recentes demonstram fragilidade na aplicação prática dessas normas, como vazamentos de dados em setores comerciais e de saúde. O estudo confirma que o enfrentamento do estelionato eletrônico exige uma abordagem multissetorial: legislação atualizada, cooperação internacional, capacitação dos operadores do direito e educação digital da população.

Conclusão

Conclui-se que o estelionato eletrônico é um dos maiores desafios contemporâneos do Direito Penal brasileiro. Apesar dos avanços legislativos e jurisprudenciais, a constante inovação tecnológica exige atualização permanente das normas e estratégias de investigação. O combate eficaz a esses delitos depende da integração entre Estado, empresas privadas e sociedade civil, aliando repressão jurídica, prevenção educativa e cooperação internacional para garantir maior segurança no ambiente digital.

Referências

BARBOSA, Cláudia Maria. Taxonomia dos Crimes Cibernéticos: Desafios e Propostas. Brasília: DEF, 2020.
BRASIL. Constituição da República Federativa do Brasil. Brasília: Senado Federal, 1988.
BRASIL. Código Penal. Decreto-Lei nº 2.848, de 7 de dezembro de 1940.
BRASIL. Lei nº 12.737/2012 (Lei Carolina Dieckmann).
BRASIL. Lei nº 12.965/2014 (Marco Civil da Internet).
BRASIL. Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD).
CAMARGO, Coriolano Almeida; SANTOS, Cleórbete. Crimes Cibernéticos: Teoria e Prática. São Paulo: XYZ, 2018.
DONEDA, Danilo; SARLET, I. W.; MENDES, L. S. Estudos sobre proteção de dados pessoais. São Paulo: Saraiva, 2022.
GOMES, Luiz Flávio. Direito Penal Brasileiro. São Paulo: XYZ, 2018.

GRECO, Rogério. Crimes Cibernéticos: Uma Nova Abordagem. Rio de Janeiro: ABC, 2019.
JESUS, Damásio de; MILAGRE, José Antônio. Manual de Crimes Informáticos. São Paulo: Saraiva, 2016.
POLÍCIA FEDERAL. Crimes Cibernéticos. Brasília: DPF, 2023.