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

DIREITO PENAL E CIBERCRIMES

D598
Direito penal e cibercrimes [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. Cibercrimes. 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.

ESTELIONATO VIRTUAL: UMA VISÃO JURÍDICA E TECNOLÓGICA DA MODERNIDADE DO CRIME

VIRTUAL EMBEZZLEMENT: A LEGAL AND TECHNOLOGICAL VIEW OF THE MODERNITY OF CRIME

Michelly Monteiro Pacheco
Lidiane Aparecida Feitoza

Resumo

Com a evolução da tecnologia e o crescimento dos usuários na internet, aumentaram os crimes praticados no ambiente virtual. São inúmeros os delitos nesse meio, mas neste artigo, estudaremos especificamente o estelionato virtual, que consiste na obtenção de vantagem ilícita mediante fraude no ambiente digital. O presente trabalho visa analisar a crescente onda do crime de estelionato virtual, a legislação brasileira vigente, os desafios enfrentados durante a investigação, a punição e as formas de prevenção. A metodologia utilizada para o desenvolvimento da pesquisa é a qualitativa, através do método dedutivo, baseado em doutrinas, artigos científicos e legislações relacionadas ao tema.

Palavras-chave: Ambiente virtual, Crimes cibernéticos, Estelionato virtual

Abstract/Resumen/Résumé

With the evolution of technology and the growth of internet users, crimes committed in the virtual environment have increased. There are countless crimes in this environment, but in this article, we will specifically study virtual fraud, which consists of obtaining an illicit advantage through fraud in the digital environment. This work aims to analyze the growing wave of the crime of virtual embezzlement, current Brazilian legislation, the challenges faced during the investigation, punishment and forms of prevention. The methodology used to develop the research is qualitative, through the deductive method, based on doctrines, scientific articles and legislation related the topic

Keywords/Palabras-claves/Mots-clés: Virtual environment, Cybercrimes, Virtual fraud

1. INTRODUÇÃO

Atualmente, o avanço tecnológico e a expansão da internet tem transformando e facilitado significativamente o cotidiano da sociedade, proporcionando inúmeras facilidades e serviços que permeiam o cotidiano dos usuários, desde o entretenimento até o trabalho. No entanto, essa evolução trouxe consigo um aumento alarmante na incidência de crimes cibernéticos, dos quais o estelionato virtual tem se destacado.

O crescimento exponencial do estelionato virtual no Brasil reflete não apenas a sofisticação dos métodos utilizados pelos criminosos, mas também os desafios enfrentados pelo sistema jurídico na investigação e punição desses delitos. A complexidade na identificação dos responsáveis, aliada à falta de recursos e capacitação adequada dos órgãos de segurança e judiciais.

Nesse contexto, esse trabalho tem como objetivo geral aprofundar e explorar o estudo sobre o crime de estelionato virtual. Para isso, será analisado as legislações brasileiras vigentes para o enfrentamento deste delito, seus aspectos tecnológicos e seus impactos sociais e econômicos dessa prática ilícita. Além disso, a pesquisa tem como objetivo específico verificar se há autocolocação da vítima nessa situação, além de ser discutido o papel crucial da conscientização, enfatizando a importância da educação digital e medidas preventivas para mitigar os riscos associados ao uso da internet.

Ademais, busca-se oferecer contribuições significativas para o entendimento e enfrentamento dessa crescente ameaça no contexto digital contemporâneo, respondendo os seguintes questionamentos: Como são investigados e punidos os criminosos que cometem o estelionato virtual? Com o crescimento exacerbado desse crime, quais são as medidas de prevenção?

Outrossim, a metodologia utilizada para o desenvolvimento do trabalho é a qualitativa, de cunho bibliográfico documental, por meio do método dedutivo, onde é realizado um estudo embasado em doutrinas, artigos científicos, legislações pertinentes ao estudo, que fornecerem subsídios concretos a pesquisa.

2. DESENVOLVIMENTO

CAPITULO I

É notório o avanço da tecnologia e, consequentemente, o aumento do número de usuários na internet, que buscam inúmeras funcionalidades e facilidades para o cotidiano, como o entretenimento, notícias, comunicação, serviços bancários e de consumo.

A pandemia da Covid-19 foi um marco de grandes transformações e adaptações no comportamento dos usuários, onde se viram praticamente obrigados a aderir um maior uso da internet, em razão das regras sanitárias.

Em consequência desta ampliação de transações via internet, aumentou-se também a quantidade de delitos praticados no ambiente virtual. São diversas as práticas criminosas ocorridas no ambiente digital, que vão desde a pornografia infantil, sequestro de dados, golpes envolvendo PIX até o estelionato virtual.

O crime de estelionato encontra-se tipificado no artigo 171 do Código Penal e consiste no ato de obter vantagem ilícita, mediante a utilização de artifícios ardilosos e fraudulentos, colocando a vítima em situação vulnerável de erro, ressalta-se que a vítima é enganada. O estelionato pode ser praticado também no ambiente virtual, conhecido, portanto, como "estelionato virtual", também previsto no §2º A do mesmo artigo.

O estelionato virtual pode ocorrer de diversas maneiras, como uso de sites falsos, recebimento de links, e-mails, SMS encaminhados para a vítima com mensagens atrativas, despertando a curiosidade, oportunidade e até mesmo, o medo na vítima, fazendo com que ela clique nos links, gere cadastros com a inserção de dados pessoais, senhas e números de cartão de crédito.

Considerado como o "crime da moda" o estelionato no Brasil cresceu de forma exponencial nos últimos cinco anos. Somente no ano de 2022, foram registrados 1.819.409 casos do crime, correspondendo 326% a mais que em 2018, que na época ocorreram 426.799 registros, segundo pesquisa realizada pelo Fórum Brasileiro de Segurança Pública, divulgada no Anuário Brasileiro de Segurança Pública em 2023.

CAPÍTULO II

Sabe-se que a punição de crimes cibernéticos é um grande desafio para o ordenamento jurídico brasileiro, em razão da complexidade na investigação, comprovação e identificação dos responsáveis. A quantidade de crimes e processos no país contribui para a morosidade no Poder Judiciário, exacerbada pela falta de recursos e capacitação adequada nos órgãos investigativos e judiciais. Essa realidade resulta em lentidão na cooperação e, muitas vezes, culmina na impunidade dos criminosos que atuam no ambiente virtual, como o estelionato virtual.

A investigação de crimes cibernéticos geralmente inicia-se pela identificação do Internet Protocol (IP) de origem e de vinculação do usuário responsável, que envolve

localizar sistemas informáticos e coletar as provas da conduta ilícita. No entanto, muitos criminosos utilizam técnicas que ocultam sua identidade, como redes privadas virtuais (VPNs) e proxies, ocasionando ainda mais dificuldade no processo investigativo. Além disso, as investigações precisam ser conduzidas com muita cautela para garantir a integridade das provas digitais, evitando qualquer contaminação que possa invalidá-las.

A vulnerabilidade a esses crimes tem aumentado consideravelmente, e um aspecto pouco abordado, porém crucial, é a contribuição involuntária das vítimas no crime de estelionato virtual. Muitas vezes criminosos conseguem consumar seus golpes devido a "colaboração" das vítimas por meio de ações, como o fornecimento de informações pessoais a websites não confiáveis, que facilitam a prática criminosa.

Nesse sentido, é imperioso alegar e reconhecer a participação da vítima, que é responsável por proteger seus próprios direitos legais e dados. Ao fornecer informações pessoais a sites ou pessoas não confiáveis a vítima está aceitando os riscos da sua conduta. Esses riscos não inevitavelmente resultarão em danos aos direitos legais fundamentais, como autodeterminação informática ou patrimônio, mas podem levar ao seu exercício com responsabilidade própria.

CAPÍTULO III

O estelionato virtual representa uma ameaça significativa no atual cenário jurídico, o que exige medidas, abordagens e estratégias preventivas a esse tipo de crime, visando mitigar os riscos e proteger os usuários no ambiente virtual.

Nesse sentido, a educação digital desempenha um papel crucial na prevenção do estelionato virtual. Os usuários precisam ser conscientizados sobre as principais práticas utilizadas pelos criminosos, como phishing, sites falsos, fraudes bancárias (falso funcionário, falso motoboy), clonagem de whatsapp, boletos falsos, dentre outros. Campanhas educativas podem alertar sobre os sinais de fraude online, incentivando práticas seguras de navegação e transação na internet. Educar os usuários desde cedo, nas escolas e em programas de formação profissional, pode fortalecer a resistência contra golpes virtuais e promover uma cultura de segurança digital.

A implementação de medidas de segurança robustas é essencial para proteger os usuários contra o estelionato virtual. Empresas e instituições financeiras devem adotar tecnologias de autenticação multifatorial, criptografia de dados e sistemas de detecção de

fraudes avançados. A atualização regular de software e a utilização de firewalls e antivírus são práticas básicas que ajudam a reduzir vulnerabilidades.

Além disso, a criação e implementação de políticas públicas e regulamentações específicas são fundamentais para combater o estelionato virtual. É necessário fortalecer a legislação existente e desenvolver novas leis que abordem os desafios emergentes no ambiente digital. Isso inclui a colaboração entre governos, setor privado e sociedade civil para criar um ambiente regulatório que incentive a segurança cibernética e responsabilize os infratores.

3. CONCLUSÃO

Conclui-se que com o avanço tecnológico e a expansão da internet, embora tenham proporcionado inúmeras facilidades e transformado significativamente o cotidiano da sociedade, também trouxeram consigo desafios consideráveis, especialmente no campo dos crimes cibernéticos. Este trabalho abordou de forma aprofundada o crime de estelionato virtual, analisando a sofisticação dos métodos utilizados pelos criminosos, a complexidade enfrentada pelo sistema jurídico na investigação e punição desses delitos, e os impactos sociais e econômicos dessa prática ilícita.

A pesquisa revelou que a identificação e a responsabilização dos responsáveis por estelionato virtual são dificultadas pela complexidade técnica e pela falta de recursos e capacitação adequada dos órgãos de segurança e judiciais.

Além disso, foi destacado o papel crucial da conscientização e da educação digital na prevenção do estelionato virtual. A autocolocação das vítimas em situações de risco, muitas vezes devido à falta de conhecimento sobre práticas seguras na internet, reforça a importância de campanhas educativas e medidas preventivas que podem mitigar significativamente os riscos associados ao uso da internet.

Em suma, combater o estelionato virtual requer uma abordagem multifacetada, que inclui aprimoramento legislativo, capacitação dos órgãos responsáveis, e, principalmente, a educação e conscientização dos usuários. Somente com um esforço integrado e contínuo de todos os setores da sociedade será possível mitigar os impactos desse crime e proteger os usuários no ambiente digital.

4. REFERÊNCIAS

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **17º Anuário Brasileiro de Segurança Pública**. São Paulo: Fórum Brasileiro de Segurança Pública, 2023. Disponível em https://forumseguranca.org.br/wp-content/uploads/2023/07/anuario-2023.pdf. Acesso em 07 de jul. de 2024.

CRUZ, Diego; RODRIGUES, Juliana. **Crimes Cibernéticos e a Falsa Sensação de Impunidade.** Revista Científica Eletrônica do Curso de Direito, 13ª Edição. Janeiro 2018. Disponível em: https://faef.revista.inf.br/imagens_arquivos/arquivos_destaque/iegWxiOtVJB1t5C_2019-2-28-16-36-0.pdf. Acesso em: 07 de julho de 2024.

DIAS, Vera Marques. **A Problemática da Investigação do Cibercrime.** Data Venia - Revista Jurídica Digital. P. 74-76. Disponível em: https://www.datavenia.pt/ficheiros/pdf/datavenia01.pdf. Acesso em: 07 de julho de 2024.

MACHADO, Daniela Regina Gabriel. **ESTELIONATO VIRTUAL: uma análise da prática e repressão desse crime.** 2022.Revista Científica Multidisciplinar do CEAP. Disponível em http://periodicos.ceap.br/index.php/rcmc/article/view/149/92. Acesso em 07 de jul. de 2024.

MELO, Mylena Ketley Borges. **Um estudo sobre o estelionato virtual e o impacto da superexposição de dados.** 2022. Centro Universitário do Planalto Central Apparecido dos Santos – Uniceplac. Disponível em https://dspace.uniceplac.edu.br/bitstream/123456789/2155/1/Mylena%20Ketley%20Borges%20de%20Melo.pdf. Acesso em 07 de jul. de 2024.

SILVA, Cristian Renner Virginio da. **A CONDUTA DA VÍTIMA NO DELITO DE ESTLIONATO VIRTUAL: uma análise à luz da teoria da imputação objetiva de Claus Roxin.** Disponível em: https://repositorio.ufpb.br/jspui/bitstream/123456789/29395/1/CRVS08112023.pdf. Acesso em: 08 de jul. de 2024.