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.

CIBERCRIMINALIDADE: UMA ANÁLISE DO ROUBO DE DADOS NA APLICAÇÃO DE GOLPES VIRTUAIS SOB A PERSPECTIVA DO MARCO CIVIL DA INTERNET

CYBERCRIMINALITY: AN ANALYSIS OF DATA THEFT IN THE APPLICATION OF VIRTUAL SCAMS FROM THE PERSPECTIVE OF THE MARCO CIVIL DA INTERNET

Mirella Negreiros Rodrigues
Eduarda Tierno Ribeiro

Resumo

Este estudo investiga crimes cibernéticos, especialmente o roubo de informações para fins fraudulentos, à luz do Marco Civil da Internet brasileiro. Examina como essas práticas desafiam conceitos éticos e legais, como vazamentos de dados contribuem para fraudes online, os métodos dos cibercriminosos, a responsabilidade dos provedores de Internet na proteção de dados, as sanções criminais e as medidas preventivas. A análise questiona as normas entre direito digital, direito penal e o submundo do crime na Internet, explorando a atuação da Lei do Marco Civil da Internet nesse cenário criminoso.

Palavras-chave: Cibercriminalidade, Roubo, Golpes, Internet

Abstract/Resumen/Résumé

This study investigates cybercrimes, particularly the theft of information for fraudulent purposes, in light of the Brazilian Internet Civil Framework. It examines how these practices challenge ethical and legal concepts, how data leaks contribute to online fraud, the methods used by cybercriminals, the responsibility of Internet service providers in protecting data, criminal sanctions, and preventive measures. The analysis questions the norms between digital law, criminal law, and the underworld of Internet crime, exploring the role of the Internet Civil Framework Law in this criminal scenario.

Keywords/Palabras-claves/Mots-clés: Cybercrime, Theft, Scams, Internet

1. Introdução

O cibercrime tornou-se um problema crescente num mundo cada vez mais digitalizado, apresentando desafios complexos que ultrapassam fronteiras éticas e legais. Neste contexto, o roubo e a fraude de dados aparecem como uma prática importante que está afetando tanto indivíduos como organizações.

Porém, do ponto de vista provocativo, roubar dados para o uso de fraudes, desafia normas em um campo complexo entre o direito digital, o direito penal e o submundo do crime cibernético.

O problema de pesquisa se concentra na necessidade de enfrentar os desafios impostos pela cibercriminalidade, questionando de que forma as práticas criminosas online estão redefinindo conceitos éticos e legais, e como o vazamento de dados pessoais contribui para fraudes virtuais. O objetivo principal é analisar o roubo de dados utilizado em golpes, explorando as consequências éticas, jurídicas e sociais, os métodos utilizados pelos criminosos, a responsabilidade penal dos provedores de serviços online, além das medidas preventivas e sanções aplicáveis.

A metodologia adotada é de caráter analítico e dedutivo, baseada em uma revisão bibliográfica que inclui livros, atos normativos e artigos científicos, além da análise das leis e jurisprudências relevantes, como a Lei Geral de Proteção de Dados (LGPD). Esta pesquisa busca contribuir para a construção de um ambiente digital mais ético e resistente às ameaças cibernéticas, oferecendo soluções práticas e teóricas para os desafios identificados.

2. Desenvolvimento

A cibercriminalidade tem se tornado uma preocupação crescente em um mundo cada vez mais digitalizado, apresentando desafios complexos que transcendem fronteiras éticas e legais. Dentro deste contexto, o roubo de dados para golpes virtuais surge como uma prática significativa, afetando tanto indivíduos quanto organizações. Esta pesquisa propõe uma análise provocadora sobre o roubo de dados para golpes, desafiando normas no intricado campo entre direito digital, direito penal e os submundos do crime online.

2.1) Capítulo 1: Cibercriminalidade e Marco Civil da Internet

Os crimes digitais são uma série de atividades ilegais conduzidas na web e lançam a gamas de ações de sistema furtos de equipamentos online e roubos de identificação. Um tipo comum de prisão furtiva usado neste campo é o uso de dados. Logo, nos aspectos iniciais, os ladrões se atualizaram e começaram a incluir métodos de engenharia social, táticas antifraude e malware.

Os criminosos virtuais roubam registros comprovados para praticar traz contração financeira e coerção ou espionagem entre as vítimas selecionadas. A falta de identificação e captura de fita de criminoso auxilia nesta furtos.

Ademais a conexão mundial é talvez a maior concordância adicional, pois os infiltrados podem agir de qualquer lugar e os servidores e vários registros de vítimas estão em diferentes perder, Da mesma forma, identificar esses malfeitores ou relação junto com o mundo internacional é mais desafiador.

2.2) Capítulo 2: Sanções Aplicáveis

Sanções Aplicáveis: Análise das sanções legais aos criminosos.

É inevitável procurar táticas para impedir esses impasses devido à ameaça séria que representam para a economia, a privacidade e a segurança se seus cidadãos, as violações de cibersegurança, pois os crimes cibernéticos e roubos de identidade estão se tornando uma das principais preocupações das leis ao redor do mundo.

Para combater esses desafios, muitas leis impõem várias sanções aos criminosos. Uma das medidas mais importantes é a reclusão. Dependendo da gravidade do delito, os indivíduos culpados pela invasão do sistema podem pegar prisão por meses a anos, enquanto pessoas responsáveis por fraudes em grande escala ou atividades de hacking podem ser presas por mais de uma década. Além disso, muitos criminosos são multados. Vale ressaltar que a quantidade de dinheiro depende da natureza do crime e do dano causado ou do lucro obtido ilegalmente.

Outra medida importante é a restituição e a compensação. Muitas leis exigem que criminosos devolvam o dinheiro obtido durante a violação e compensem as vítimas pelo sofrimento. Além disso, os tribunais podem impor certas restrições ao envolvimento futuro dos criminosos nas atividades do ciberespaço.

2.3) Capítulo 3: Caso de Vazamento de Dados: Estudo de um caso real e suas

consequências.

Vazamento de Dados da Equifax.

Ao analisar o caso do vazamento de Dados da Equifax, a Equifax, uma das maiores agências de crédito dos EUA, sofreu um dos maiores hackers de segurança da informação na história 2017. Onde os hackers exploraram uma vulnerabilidade em seu sistema, resultando no comprometimento de informações detalhadas para aproximadamente 147 milhões de pessoas. Mais especificamente, os hackers obtiveram os nomes dos clientes, números do Seguro Social, datas de nascimento e, ocasionalmente, informações da carteira de motorista e cartão de crédito. As consequências desse ataque foram imediatas e devastadoras para os clientes envolvidos. Com um risco muito maior de roubo de identidade e fraude financeira, a maioria das partes afetadas sentiu os efeitos do hackeamento. A quebra da confiança pública na Equifax, que durou quase dois meses após o vazamento, não era um santo, e ações perdiam valor, o que sugeriria uma quebra da confiança do acionista com a empresa.

Do ponto de vista legal, a Equifax teve que pagar várias ações e foi multada pelo escândalo. Os acordos com a Comissão Federal de Comércio dos Estados Unidos e outras entidades totalizaram até 700 milhões de dólares, que a empresa concordou em pagar.

3. Objetivos

O objetivo geral tem como base analisar o roubo de dados para golpes no contexto do estelionato online, explorando as consequências éticas, jurídicas e sociais. Serão estudados os principais métodos utilizados pelos criminosos cibernéticos nessa prática.

Será examinada a responsabilidade penal dos provedores de serviços online diante do vazamento de dados de seus usuários, investigando também as estratégias dos criminosos online e os esforços das autoridades e da população em geral para combater essas práticas. Pretende- se compreender as sanções aplicáveis aos criminosos e as medidas que as autoridades jurídicas devem adotar para prevenir e combater tais estratégias.

Por fim, busca-se verificar soluções para essa questão, utilizando como base teórica e exemplos práticos os conceitos éticos e legais pertinentes, visando contribuir para a construção de um ambiente digital mais ético e resiliente às ameaças cibernéticas.

Assim, desenvolve-se os objetivos específicos que vão analisar como ocorre o roubo de dados e a captura dos dados vazados, compreender a dinâmica do golpe utilizado para roubo de dados e aplicação do estelionato com base no vazamento de dados, analisando as sanções

aplicáveis aos criminosos e as medidas que as autoridades jurídicas devem adotar para prevenir e combater tais estratégias. Onde reside as indispensáveis necessidades de compreender e afrontar os desafios impostos pela cibercriminalidade em um mundo cada dia mais digitalizado. No entanto, muitas das vezes, as abordagens convencionais para lidar com o impasse não são suficientes, visto que não conseguem concorrer com a rápida evolução das técnicas criminosas nos submundos da internet.

4. Métodos

Para a presente pesquisa, adotado o método analítico e dedutivo, com a finalidade de alcançar o foco da investigação, buscando, dentro da aptidão humana, a verdade ou, mais precisamente, afirmações verídicas.

Dessa maneira, uma das técnicas realizadas em nossa pesquisa será a investigação bibliográficas, com menções já consideradas sejam essas feitas por meio escrito ou digital, como livros, atos normativos e artigos científicos, desenvolvendo por meio de doutrinas e

Ademais ferramentas para conceitualizar e analisar a Lei N° 12.946 e as demais referencias para o prosseguimento das investigações.

5. Desenvolvimento da pesquisa

Primeiramente foi realizada uma revisão bibliográfica a respeito da cibercriminalidade nas bases pesquisas bibliográficas. Na sequência foi feito uma busca de dados por meio de livros e sites com estatísticas. Para analisar os desafios na era digital com fulcro na Lei de Proteção de Dados (LGPD) e utilizado o entendimento de Leis e Jurisprudências referente ao estudo. A análise dos dados com base no crescimento acelerado da internet e o uso irresponsável dela, e como as práticas criminosas on-line desafiam e redefinem conceitos éticos e legais e como o vazamento de dados pessoais contribui para a ocorrência de dados de estelionato on-line.

6. Resultados da discussão

Esta pesquisa, residiu nas indispensáveis necessidades de compreender e combater os desafios impostos pela cibercriminalidade em um mundo cada dia mais digitalizado. No entanto, percebemos que muitas das vezes, as abordagens convencionais para lidar com o impasse são insuficientes, visto que não conseguem concorrer com a rápida evolução das técnicas criminosas nos submundos da internet.

Assim, ao desenvolver os objetivos que analisaram como ocorre o roubo de dados

e a captura dos dados vazados, compreendemos a dinâmica do golpe utilizado para roubo de dados e aplicação do estelionato com base no vazamento de dados, sob a análise das sanções aplicáveis aos criminosos e as medidas que as autoridades jurídicas adotam para prevenir e combater tais estratégias.

6. Referencias preliminares

BITTENCOURT, Rodolfo Pacheco Paula. O anonimato, a liberdade, a publicidade e o direito eletrônico. 2016, Disponível em: https://rodolfoppb.jusbrasil.com.br/artigos/371604693/o-anonimato-a-liberdade ANUÁRIO PESQUISA E EXTENSÃO UNOESC SÃO MIGUEL DO OESTEa publicidade-e-o-direito-eletronico> Acesso em: 04.abr.2024.

BRASIL. Lei 14.155 de 27 de maio de 2021. Disponível em https://www12.senado.leg.br/noticias/materias/2021/05/28/lei-com-penas-maisdurascontra-crimes-ciberneticos-e-sancionada.

Fernandes, R. (2020). Desafios legais na era digital. In: Santos, M. Tecnologia e Sociedade: Perspectivas Contemporâneas. 2ª edição. São Paulo: Editora XYZ, p. 45-68.

García, M.; Lee, S. The Impact of Data Breaches on Online Fraud: An Empirical Analysis. Journal of Cybersecurity Research, v. 5, n. 1, p. 78-92, 2019.

Moodle USP: e-Disciplinas. Disponível em: <https://edisciplinas.usp.br/pluginfile.php/5575872/mod_resource/content/1/artigo%20JEP%203.pdf>. Acesso em: 27 jun. 2024.

Oliveira, R. F.; Pereira, L. M. Impactos do Roubo de Dados na Sociedade Contemporânea. Cadernos de Pesquisa em Tecnologia da Informação, v. 15, n. 1, p. 60-75, 2019.

Silva, A. B.; Santos, C. D. Cibercrime no Brasil: Tendências e Desafios. Revista Brasileira de Segurança Digital, v. 8, n. 2, p. 30-45, 2021.

Smith, J.; Johnson, A. Cybercrime Trends: A Global Perspective. International Journal of Cybersecurity, v. 10, n. 2, p. 45-60, 2020.