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.

CRIMES DIGITAIS E ANONIMATO NA INTERNET: DESAFIOS DA INVESTIGAÇÃO CRIMINAL NO BRASIL

DIGITAL CRIMES AND ANONYMITY ON THE INTERNET: CHALLENGES OF CRIMINAL INVESTIGATION IN BRAZIL

Anelise Ribeiro da Silva
Davi Marcos Pereira da Silva

Resumo

O artigo aborda os desafios enfrentados pela investigação criminal no Brasil diante do crescente número de crimes digitais, especialmente aqueles que se aproveitam do anonimato na internet. A transformação tecnológica trouxe inúmeros benefícios, mas também abriu espaço para práticas criminosas virtuais que dificultam a atuação eficiente do sistema de justiça.

Palavras-chave: Anonimato, Investigação criminal, Crimes digitais, Ciberespaço

Abstract/Resumen/Résumé

The article addresses the challenges faced by criminal investigation in Brazil in light of the growing number of digital crimes, especially those that take advantage of anonymity on the internet. Technological transformation has brought countless benefits, but it has also opened space for virtual criminal practices that hinder the efficient operation of the justice system.

Keywords/Palabras-claves/Mots-clés: Anonymity, Criminal investigation, Digital crimes, Cyberspace

1. Introdução

A esfera digital, hodiernamente, contém uma vasta gama de ferramentas que visam facilitar e tornar mais rápido diversos tipos de processos, no entanto com a rápida evolução desse espaço digital, também surgiram rapidamente diversos problemas relacionados a segurança desses ambientes, no caso dos crimes digitais e o anonimato na internet.

Importante salientar, no que se refere ao anonimato na internet a problemática reside na dificuldade em identificar os sujeitos praticantes dos delitos na internet, consequentemente há dificuldade em obter informações mais especificas quanto a esses sujeitos. É essencial que tenha um equilíbrio à proteção de dados e direitos fundamentais (como a privacidade e a liberdade de expressão).

> "Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> IX - é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença;
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;" (BRASIL, 1988).

Assim, observa-se que há certa violação aos direitos fundamentais mencionados anteriormente, busca-se, portanto, soluções a fim de mitigar os danos causados aos usuários que venham a sofrer esses crimes digitais, onde não há uma identificação do sujeito praticante do crime virtual.

Em face ao exposto, a pesquisa tem por objetivo central mapear os impactos gerados pela ausência de regulamentação especifica para combater esses crimes digitais, além de buscar ferramentas que possam auxiliar na identificação desses usuários e consequentemente a redução do anonimato na internet.

Cumpre salientar, ainda, que a presente pesquisa foi desenvolvida através do método dedutivo, com recursos em pesquisas bibliográficas, legislativas, estudos de obras sobre as

tecnologias e sobre a responsabilidade jurídica pela falta de transparência e ética diante dos usuários que sofrem esses crimes, além de relacionar o papel da LGPD no tocante à temática.

Ademais, a caráter do Direito, a elucidação e a demonstração do art. 6° da Constituição Federal, lei suprema, em relação aos efeitos gerados pela falta de segurança no meio digital são fundamentais para a exemplificação dos direitos instituídos aos cidadãos brasileiros e as formas de sua fruição diante da problemática em questão.

2. O papel do anonimato nos crimes digitais

O anonimato digital é uma característica que permite aos usuários navegarem, interagirem e se comunicarem na internet sem que sua identidade real seja facilmente identificada. Embora o anonimato seja uma ferramenta importante para garantir a liberdade de expressão e a proteção de dados pessoais, ele também tem sido amplamente explorado por cibercriminosos.

Os autores de crimes digitais frequentemente utilizam redes privadas (VPNs), criptografia, navegadores como o Tor e outros métodos para ocultar sua identidade e localização. Isso dificulta não apenas a identificação dos criminosos, mas também a obtenção de provas digitais válidas para processos judiciais.

Há atualmente debate entre privacidade online e segurança cibernética, que se tornou central nas discussões sobre crimes digitais. De um lado, cidadãos e organizações defendem o direito ao sigilo de suas informações; de outro, autoridades clamam por mais acesso a dados e registros para efetuar investigações eficazes.

Esse dilema exige soluções equilibradas, como a criação de mecanismos legais e técnicos que permitam rastrear criminosos digitais sem comprometer os direitos de usuários comuns. A educação digital e a conscientização da população também são elementos essenciais na prevenção e no combate aos delitos virtuais.

3. A Expansão da Criminalidade Digital

É inegável que o desenvolvimento tecnológico trouxe inúmeros benefícios para sociedade contemporânea, entretanto esse avanço também originou diversos tipos de criminalidade e com ele o anonimato digital.

Esses crimes por sua vez, são velozes e quase sempre invisíveis, representando hoje, um dos maiores desafios para o sistema judiciário. O anonimato é uma prática comum em

ambientes digitais, isso porque figura imenso obstáculo na identificação de usuários criminosos.

Analisando o cenário brasileiro, a ausência de tipificação penal que especifique essa conduta criminosa, acaba contribuindo com a impunidade da prática criminal.

A criminalidade digital tem se expandido rapidamente com o avanço da tecnologia e da conectividade global, golpes virtuais, invasões de sistemas e roubos de dados pessoais tornaram-se cada vez mais frequentes. Essa expansão atinge tanto indivíduos quanto empresas, causando prejuízos financeiros e violando direitos fundamentais, a falta de fronteiras na internet favorece a atuação de criminosos em escala internacional.

É perceptível a problemática entre os dois principais valores constitucionais, a proteção à privacidade elencado no artigo 5º, incisos X e XII da CF/88 e o direito/dever que o estado tem de punir as condutas criminosas. Atualmente, a LGPD, Lei Carolina Dieckmann e o Marco Civil da Internet colaboram para a proteção desses ambientes virtuais, mas ainda carecem de efetividade investigativa.

Como exemplo disso, temos o artigo 10 do Marco Civil da Internet, que visa tratar o sigilo dos dados e a comunicação privada, de maneira a impor várias limitações ao acesso a essas informações quando na verdade essas plataformas nem possuem sede no Brasil.

Para tratar o problema é preciso tratar a causa, fazendo com que o estado invista em tecnologias que possam rastrear e analisar os dados dessas plataformas como sistemas de machine learning forense e algoritmos capazes de identificar irregularidades nos padrões dos dados. Além disso, as blockchains podem ser empregadas de maneira a garantir a integridade das provas digitais.

Destarte, entende-se que a problemática sobre os crimes digitais exige muito mais que somente a legislação. O anonimato precisa deixar de ser um escudo para a conduta criminosa digital, mas sim ajudando o sistema investigativo judicial a enfrentar os desafios impostos pela criminalidade cibernética.

4. Conclusão

A crescente incidência de crimes digitais no âmbito brasileiro, em especial aqueles que têm como base o anonimato digital, impõe de maneira indireta ao ordenamento jurídico e às instituições investigativas um dos maiores desafios presentes na era contemporânea: a investigação dos crimes digitais.

Embora para alguns o anonimato digital denote grande símbolo de liberdade proteção à privacidade, para o sistema judiciário demonstra grande urgência, visto que muitos usuários usam e exploram de maneira indevida, evidenciando medidas de políticas públicas e mecanismos jurídicos mais eficazes.

É notório, que o Brasil já demonstra grande disposição de elementos legais, entretanto ainda carece de aplicação prática que seja mais incisiva e especializada para enquadrar nas ações concretas. A ausência dessa especialização acaba ajudando a aumentar a perpetuação da impunidade.

Portanto, é indispensável que o estado invista em atualização legal mas também em recursos tecnológicos eficientes que auxiliem na rastreabilidade de condutas criminosas sem deixar de preservar os direitos fundamentais sociais.

É nessa "balança" de liberdade e segurança que surge o maior desafio da atualidade: a garantia de um espaço digital seguro, transparente e justo.

Referências

BRASIL. Constituição da República Federativa do Brasil de 1988. Diário Oficial da União, Brasília, DF, 5 out. 1988.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012 (Lei Carolina Dieckmann). Dispõe sobre a tipificação criminal de delitos informáticos. Disponível em: www.planalto.gov.br

BRASIL. Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: www.planalto.gov.br

BRASIL. Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados – LGPD). Regulamenta o tratamento de dados pessoais. Disponível em: www.planalto.gov.br

CASTRO, Rodrigo A. Crimes Cibernéticos: Desafios e Estratégias de Investigação. São Paulo: Editora Forense, 2021.

SOUZA, Mariana R. Anonimato na Internet e Direito Penal. Rio de Janeiro: Editora Jurídica, 2022.

SILVA, Renato Opice Blum; DONEDA, Danilo. A proteção dos dados pessoais na era da informação: um desafio jurídico. Revista de Direito Civil Contemporâneo, v. 7, 2021.

FERRAZ, Luciana Grassano. *Marco Civil da Internet e as demandas investigativas: limitações e soluções