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.

DESAFIOS DA COMPETÊNCIA JURISDICIONAL NO DIREITO DIGITAL BRASILEIRO: IMPLICAÇÕES LEGAIS E PRÁTICAS NOS CRIMES CIBERNÉTICOS

CHALLENGES OF JURISDICTIONAL COMPETENCE IN BRAZILIAN DIGITAL LAW: LEGAL AND PRACTICAL IMPLICATIONS IN CYBER CRIMES

Manuela Oliveira Rodrigues

Resumo

Este resumo analisa os desafios da competência jurisdicional no direito digital brasileiro, considerando as implicações legais e práticas dos crimes cibernéticos. A evolução tecnológica tem transferido conflitos para o ambiente digital, desafiando os sistemas jurídicos globais e exigindo adaptações contínuas das leis. No Brasil, a competência jurisdicional enfrenta dificuldades complexas, como a definição de jurisdição territorial e a aplicação de normas em um ambiente virtual transnacional. O estudo investiga as implicações legais e práticas dessa migração de crimes e como afeta a jurisdição, utilizando métodos dedutivos e pesquisa bibliográfica para analisar a legislação existente e casos concretos.

Palavras-chave: Competência, Cibercrimes, Direito digital, Direito penal

Abstract/Resumen/Résumé

This summary analyzes the challenges of jurisdictional competence in Brazilian digital law, considering the legal and practical implications of cyber crimes. Technological evolution has shifted conflicts to the digital environment, challenging global legal systems and requiring continuous adaptations of laws. In Brazil, jurisdictional competence faces complex difficulties, such as defining territorial jurisdiction and applying norms in a transnational virtual environment. The study investigates the legal and practical implications of this migration of crimes and its impact on jurisdiction, using deductive methods and bibliographic research to analyze existing legislation and concrete cases.

Keywords/Palabras-claves/Mots-clés: Jurisdiction, Cybercrimes, Digital law, Criminal law

Introdução

O desenvolvimento deste resumo visa analisar os desafios da competência jurisdicional no direito digital brasileiro, observando as implicações legais e práticas nos crimes cibernéticos. Com as mudanças sociais, econômicas e, principalmente, tecnológicas ocorridas na sociedade, observa-se uma migração dos conflitos para a esfera digital, reformulando conceitos jurídicos estabelecidos anteriormente.

Na era da globalização tecnológica, o surgimento de novas tecnologias e a expansão do ambiente digital têm desafiado os sistemas jurídicos em todo o mundo, demandando uma constante adaptação das leis e das práticas judiciais. No contexto brasileiro, a competência jurisdicional no âmbito do direito digital enfrenta uma série de desafios complexos, que vão desde a definição de jurisdição territorial até a aplicação efetiva das normas legais em um ambiente virtual transnacional.

A competência jurisdicional, enquanto atribuição conferida ao Estado para a resolução de conflitos, assume uma dimensão complexa no contexto digital. A transnacionalidade das comunicações, a ausência de fronteiras físicas e as peculiaridades da internet como espaço de interação e transações apresentam novos desafios à jurisdição tradicional, provocando questionamentos sobre a eficácia das normas e dos mecanismos de aplicação do Direito em um ambiente virtual.

Esta pesquisa tem como problema central: Quais são as implicações legais e práticas resultantes da migração dos crimes para o ambiente digital e como isso impacta a competência jurisdicional no Brasil?

O objetivo desta pesquisa é compreender como as transformações tecnológicas impactam a aplicação da jurisdição, identificando lacunas normativas e obstáculos práticos. Bem como, analisar os critérios de competência jurisdicional no direito digital brasileiro; verificar a aplicabilidade da legislação existente; e analisar os casos concretos da atualidade.

Primeiramente, o método de pesquisa a ser utilizado será o método dedutivo, que consiste em abordar ideias gerais sobre determinado tema a fim de obter conclusões particulares sobre o mesmo, segundo o dicionário Michaelis (2015, S.I) “dedução é um modo ou processo de raciocinar, partindo de uma ou várias proposições

consideradas verdadeiras e que encerram uma evidência". Em seguida, fazer-se-á uso da pesquisa bibliográfica, examinando doutrinas, artigos científicos, legislações e jurisprudências. Bem como, a análise de casos nacionais do âmbito digital.

Competência jurisdicional no direito digital brasileiro

A internet trouxe consigo o aumento de crimes ocorridos no ambiente virtual, afetando tanto bens jurídicos tradicionalmente protegidos quanto novos bens jurídicos que foram recentemente regulamentados para sua proteção. Não se pode ignorar que o ambiente virtual facilita um certo grau de anonimato para aqueles que buscam cometer crimes, já que uma pessoa pode realizar atividades criminosas em um dispositivo localizado em qualquer parte do território nacional, e até mesmo ultrapassar fronteiras, atingindo outras nações. Isso demanda a colaboração de todos os países afetados pela prática criminosa para garantir a efetiva punição do criminoso. (Silva, 2015, s.i.)

Segundo Santos (2021, s.i.), a acessibilidade econômica do ciberespaço se deve ao fato de que apenas um computador com acesso à internet e motivação são os únicos requisitos necessários para que indivíduos ou organizações possam ingressar e potencialmente realizar ataques, participando assim de conflitos de importância nacional e internacional.

A verificação da competência territorial destes conflitos tem de ser feita embasada em outras fontes do direito, visto que, as lacunas da legislação brasileira não indicam como serão feitas as determinações de competência para a resolução das lides digitais. (Silva, 2015, s. i.)

O maior problema reside no caráter internacional da rede, pois a competência para julgar ações penais no âmbito da informática deve considerar o local e a jurisdição onde o crime foi cometido. Devido ao fato de que a internet não tem fronteiras, algo que seja postada nela estará acessível da mesma forma em todo o mundo. A regra para a determinação da competência é baseada no local onde a conduta se consumou, ou, em caso de tentativa, no local onde o último ato de execução foi praticado, conforme bem afirma o artigo 70 do Código de Processo Penal. (Silva, 2015, s. i.)

Sendo assim, a questão da competência será resolvida quando a máquina utilizada pelo criminoso é localizada. No entanto, é importante salientar que, nos casos em que o local da consumação não seja conhecido, a regra secundária para fixar a competência é o domicílio ou residência do réu, conforme o artigo 72 e o § 1º, do Código de Processo Penal, a competência será estabelecida pela prevenção no caso de o réu residir em mais de um local. (Silva, 2015, s. i.) (Brasil, 1941)

No que tange aos crimes à distância, ou seja, nos casos em que um crime for cometido em território nacional e o resultado ocorre em outro país, aplica-se a teoria da ubiquidade, conforme previsto no artigo 6º do Código Penal. O foro competente para julgar a ação será tanto o local onde foi realizada a ação ou omissão quanto o local onde se produziu o resultado. Assim, o foro competente será o local onde foi praticado o último ato de execução no Brasil (art. 70, §1º), ou o local no estrangeiro onde se produziu o resultado. (Silva, 2015, s. i.) (Brasil, 1940) (Brasil, 1941)

Assim sendo, para determinar a competência de acordo com a lei processual penal brasileira, são necessários alguns critérios mencionados. A determinação da competência para análise processual e o consequente julgamento dessas práticas delitivas é uma tarefa complexa devido à deficiência do sistema nacional de repressão aos crimes cibernéticos. A questão da competência para julgamento será resolvida aplicando a regra geral prevista no artigo 70, quando for possível identificar onde se encontra o dispositivo do qual partiu a conduta criminosa e onde esta se consumou. Caso contrário, essa regra será afastada e as outras regras de caráter subsidiário serão aplicadas.

A aplicabilidade da legislação brasileira nos cibercrimes

No Brasil, a legislação tem avançado para tentar acompanhar as mudanças tecnológicas e oferecer um marco legal adequado para o combate a essas novas formas de criminalidade.

A regulamentação é feita por meio de algumas legislações vigentes, sendo elas, a Lei nº 12.965/2014, um dos principais pilares da legislação brasileira sobre o uso da internet, o Marco Civil da Internet, estabelecendo princípios, garantias, direitos e

deveres para o uso da internet no Brasil, bem como diretrizes para a atuação do estado. Embora não seja uma lei penal, cria um ambiente regulatório que afeta diretamente o tratamento dos cibercrimes, principalmente no que diz respeito à proteção da privacidade, à neutralidade da rede e à responsabilidade dos provedores de serviços de internet. (Mendes; Branco, 2023, p. 3399, 3401)

Por conseguinte, segundo Bortot (2017, s. i.), a Lei nº 12.737/2012, conhecida como "Lei Carolina Dieckmann", foi um marco importante na tipificação dos crimes cibernéticos no Brasil, alterando o Código Penal para incluir artigos que tratam especificamente de delitos cometidos no ambiente digital, como a invasão de dispositivos informáticos (art. 154-A), que prevê penas para quem invade dispositivo alheio para obter, adulterar ou destruir dados sem autorização. Bem como, O Código Penal brasileiro tipifica uma variedade de crimes cibernéticos, principalmente após as modificações feitas pela Lei no 12.737/2012. Além disso, o Código de Processo Penal estabelece os padrões para a investigação e o processamento desses crimes.

Portanto, apesar dos avanços legislativos, o sistema de repressão aos crimes cibernéticos no Brasil ainda apresenta deficiências, visto que, investigação desses crimes requer uma infraestrutura tecnológica avançada e cooperação internacional eficaz, já que muitas vezes os dados e os criminosos se encontram em diferentes países.

Análises aos casos concretos de cibercrimes no Brasil

Os cibercrimes, devido à sua natureza transnacional e complexa, frequentemente envolvem múltiplas jurisdições, o que pode resultar em conflitos de competência. Analisar-se-á alguns casos notórios de cibercrimes no Brasil, destacando as peculiaridades de cada um e as implicações legais envolvidas.

1. Caso Lava Jato e Operações de Hacking (2019): Em 2019, hackers invadiram os dispositivos móveis de diversas autoridades envolvidas na Operação Lava Jato, incluindo o então Ministro da Justiça, Sérgio Moro. As conversas vazadas foram divulgadas pelo site The Intercept Brasil, causando um grande impacto político e jurídico. O conflito de competência surgiu porque as vítimas e os hackers estavam localizados em diferentes estados e, possivelmente, em diferentes países. Além disso,

os crimes afetaram figuras públicas de alta relevância, adicionando uma camada de complexidade ao caso.

O Tribunal Regional Federal da 1ª Região (TRF-1) decidiu que a competência para julgar o caso deveria ser da Justiça Federal em Brasília, dado o impacto nacional e a relevância dos envolvidos. A decisão levou em consideração a abrangência e a gravidade do caso. (RF-1 - Conflito de Competência n. 1042829 36.2019.4.01.0000/DF)

2. Caso Banco Neon (2018): Em 2018, o Banco Neon sofreu um ataque cibernético que resultou no vazamento de dados pessoais de milhares de clientes. Os hackers acessaram informações sensíveis, incluindo dados bancários e pessoais, que foram utilizados para realizar transações fraudulentas. Neste caso, os ataques afetaram clientes de várias regiões do Brasil e os hackers operavam a partir de diferentes estados. À vista disso, a localização das vítimas e a dispersão dos servidores comprometidos adicionaram complexidade ao caso.

A investigação inicial foi conduzida pela Polícia Federal, que posteriormente transferiu partes do caso para a Justiça Estadual de São Paulo, onde estava localizada a sede do Banco Neon. No entanto, a coordenação entre as jurisdições estadual e federal foi necessária para resolver o conflito de competência. (TRF-3 - Conflito de Competência n. 5004327-27.2018.4.03.6100/SP)

3. Caso Correios (2016): Em 2016, um grupo de hackers realizou ataques cibernéticos contra os sistemas dos Correios, obtendo acesso a dados pessoais de clientes e utilizando essas informações para fraudes postais e financeiras. O Superior Tribunal de Justiça (STJ) decidiu que a competência deveria ser da Justiça Federal, devido à natureza da empresa envolvida (Correios, uma empresa pública federal) e ao alcance nacional dos ataques. Esta decisão garantiu uma abordagem mais unificada e coordenada da investigação. (STJ - Conflito de Competência n. 140.189 - DF (2016/0145679-8))

Os casos apresentados demonstram a complexidade dos cibercrimes e os frequentes conflitos de competência que surgem devido à natureza difusa e transnacional desses crimes. A legislação brasileira, juntamente com decisões judiciais, tem buscado soluções para esses conflitos, mas ainda há desafios significativos na coordenação entre diferentes jurisdições e na aplicação eficaz da lei.

Conclusão

Devido à incapacidade do sistema nacional de repressão aos crimes cibernéticos, é uma tarefa difícil determinar quem é competente para realizar a análise processual e julgamento dessas práticas delitivas. No entanto, quando for possível identificar onde se encontra o dispositivo de origem da conduta criminosa e onde esta se consumou, a questão da competência para julgamento será resolvida aplicando a regra geral prevista no artigo 70. Caso contrário, essa regra será afastada e aplicadas as outras regras de caráter subsidiário.

Portanto, apesar dos avanços legislativos, o sistema de repressão aos crimes cibernéticos no Brasil ainda apresenta deficiências, visto que, investigação desses crimes requer uma infraestrutura tecnológica avançada e cooperação internacional eficaz, já que muitas vezes os dados e os criminosos se encontram em diferentes países.

Por fim, considerando os casos apresentados, compreende-se a complexidade dos cibercrimes e os frequentes conflitos de competência decorrentes da natureza difusa e transnacional desses crimes. A legislação brasileira, juntamente com decisões judiciais, tem buscado soluções para esses conflitos, mas ainda há desafios significativos na coordenação entre diferentes jurisdições e na aplicação eficaz da lei.

Em síntese, a migração dos crimes para o ambiente digital exige um constante aprimoramento das legislações e das práticas jurídicas para lidar com as novas realidades. No Brasil, isso implica em uma adaptação contínua das normas jurídicas e um fortalecimento das capacidades técnicas e de cooperação internacional para garantir uma resposta eficaz aos desafios impostos pelos crimes digitais.

Referências

Michaelis Dicionário Brasileiro da Língua Portuguesa. São Paulo: Editora Melhoramentos Ltda., 2015. Disponível em: https://michaelis.uol.com.br/palavra/w58D/dedu%C3%A7%C3%A3o/. Acesso em: 09 jun. 2024.

Penal, BRASIL. Decreto-Lei nº 3.689, de 3 de outubro de 1941. 0001. Código de Processo Rio de Janeiro, 3 out. 1941. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 23 jun. 2024.

SILVA, Patrícia Santos da. Direito e Crime Cibernético: análise da competência em razão do lugar no julgamento de ações penais. Brasília: Vestnik, 2015. 104 p.

SANTOS, Ilana Danielle Soares. Conflitos cibernéticos: a ascensão do ciberespaço segundo a produção científica de relações internacionais indexada na web of science. 2021. 25 f. Dissertação (Mestrado) - Curso de Relações Internacionais, Instituto de Relações Internacionais, Universidade de Brasília, Brasília, 2021. Disponível em: http://www.realp.unb.br/jspui/handle/10482/41940. Acesso em: 23 jun. 2024.

BRASIL. Congresso. Senado. Constituição (1940). Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. Rio de Janeiro, RJ, 7 dez. 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 24 jun. 2024.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. Curso de Direito Constitucional. 18. ed. São Paulo: Saraiva, 2023. 5819 p. Disponível em: https://bds.minhabiblioteca.com.br/epub/418ee60d-5047-4acc-b6cf 8f2c9ceadd62?title=Curso%20De%20Direito%20Constitucional. Acesso em: 24 jun. 2024. BORTOT, Jessica Fagundes. Crimes Cibernéticos: aspectos legislativos e implicações na persecução penal com base nas legislações brasileira e internacional. Virtuajus, Belo Horizonte, v. 2, n. 2, p. 338-362, 01 jan. 2017. Semestral. Disponível em: https://egov.ufsc.br/portal/sites/default/files/crimes_ciberneticos_aspectos_legislativos _e.pdf. Acesso em: 25 jun. 2024.