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.

RESPONSABILIDADE PENAL E OS CRIMES COMETIDOS ATRAVÉS DA INTERNET: UMA ANÁLISE DA LEGISLAÇÃO BRASILEIRA PERANTE OS CIBERCRIMES E A LEI Nº 12.737/2012 (LEI CAROLINA DIECKMANN).

CRIMINAL LIABILITY AND CRIMES COMMITTED OVER THE INTERNET: AN ANALYSIS OF BRAZILIAN LEGISLATION REGARDING CYBERCRIMES AND LAW NO. 12,737/2012 (CAROLINA DIECKMANN LAW).

Miguel Teles Nassif [1]
Mateus Augusto Aguiar Félix [2]
Matheus Henrique de Almeida Silva [3]

Resumo

O presente trabalho científico busca traçar a responsabilidade penal perante os crimes cometidos na esfera virtual, denominados como cibercrimes. A Lei n.º 12.737/2012 visa combater crimes cibernéticos no Brasil, como violação e exposição pública de dados pessoais dos indivíduos. A aplicabilidade de tal norma frente a era digital enfrenta nuancias significativas que dificultam a identificação e responsabilização dos criminosos, além de ser abrangido ao direito internacional. Para tanto, será utilizado o método dedutivo, visando demonstrar através do transcorrer histórico social, através de diversas premissas e comparações sob os casos de crimes cometidos na internet.

Palavras-chave: Responsabilidade penal, Cibercrimes, Direito penal, Lei nº 12.737/2012, Era digital

Abstract/Resumen/Résumé

This scientific work seeks to outline criminal responsibility for crimes committed in the virtual sphere, known as cybercrimes. Law No. 12,737/2012 aims to combat cybercrime in Brazil, such as violation and public exposure of individuals' personal data. The applicability of such a standard in the digital era faces significant nuances that make it difficult to identify and hold criminals accountable, in addition to being covered by international law. To this end, the deductive method will be used, aiming to demonstrate through the course of social history, through various premises and comparisons in cases of crimes committed on the internet.

Keywords/Palabras-claves/Mots-clés: Criminal liability, Cybercrimes, Criminal law, Law no. 12,737/2012, Digital age

[1] DISCENTE DO CURSO DE DIREITO DA FACULDADE DE DIREITO DE FRANCA.

[2] DISCENTE DO CURSO DE DIREITO DA FACULDADE DE DIREITO DE FRANCA.

[3] DISCENTE DO CURSO DE DIREITO DA FACULDADE DE DIREITO DE FRANCA.

1 INTRODUÇÃO

Na atualidade, a sociedade vive-se a chamada Era da Informação, a qual é derivada das diversas transformações tecnológicas decorrentes dos avanços nas relações tecnológicas e na disseminação de informações em meios de comunicações, especialmente no âmbito da sistematização de dados pessoais. Todavia, percebe-se que ainda há nuncias para garantir a segurança à toda população, visto que os crimes cometidos em tal esfera ainda são indevidamente combatidos.

Nesse afinamento, a alta demanda de digitação e fácil comunicação e acesso a informações expôs indivíduos, sociedades e governos a novas maneiras de delitos, denominados como cibercrimes. Buscando o combate a tais ameaças, a resposta legislativa se tornou indiscutível, cominando para criação de leis que visam enfrentar e responsabilizar as transgressões praticadas através do ambiente digital. Na Federação Brasileira, a Lei n.º 12.737, promulgada no ano de 2012, tornou um marco de extrema importância na busca de combater os crimes cibernéticos.

A Lei Carolina Dieckmann foi decretada no Ordenamento Jurídico Brasileiro em um ambiente de crescentes preocupações em relação com a segurança dos dados pessoais na Internet. Seu nome popular se originada de um crime que envolveu a atriz global Carolina Dieckmann, onde suas fotos pessoais foram indevidamente acessadas por hackers e divulgados nas redes sociais no ano de 2011. O presente caso aderiu grande viabilidade e repercussão dos veículos mediáticos, devida a vulnerabilidade que os indivíduos estavam sujeitos diante dos diversos ataques cibernéticos, evidenciando a extrema necessidade de uma norma que visasse punir tais delitos. Seu vigor entrou no ano de 2013 e conduziu significativas mudanças sob o Ordenamento Penal Brasileiro, onde houve a inclusão da criminalização das invasões de dispositivos celulares ou informáticos, com o objetivou ou não de haver alguma obtenção de alterar ou divulgar dados ou informações pessoais sem autorização expressa do titular.

Sob este prisma, necessário torna-se a lançar luzes do conhecimento jurídico a importância de uma legislação, pois a falta de políticas públicas de visem assegurar aos indivíduos e na tentativa de cobrir as lacunas existentes em relação aos cibercrimes. Tal feito antes de sua promulgação, carecia de leis especificas que pudessem tratar de tais delitos cometidos na esfera digital, o que dificultava a condenação dos responsáveis por tais feitos.

Ao analisar no cenário brasileiro, percebe-se certos impasses importantíssimos na efetivação de normas constitucionais e de legislações que abarcam a temática, onde uma das

maiores adversidades para a devida efetivação é a anonimidade que proporciona a Internet, a qual dificulta a devida identificação dos autores de tais crimes. Os infratores utilizam das diversas ferramentas e técnicas rebuscadas que visam ocultar a identidade e atalhar a rastreabilidade de suas redes privadas e de suas ações.

Nota-se, que a capacitação técnica e de certos recursos disponíveis para as autoridades que combatem e encarregadas de investigar tais crimes são cruciais para a devida efetividade de norma, uma vez que ante a dificuldade encontrada ao instrumentalizar as novas tecnologias notório é a posição de vulnerabilidade virtual imposta para todos os indivíduos.

Igualmente, a necessidade de coparceira internacional no combate aos cibercrimes torna-se essencial, visto que muitos dos autores de tais crimes operam e trabalhar sobre diferentes jurisdições, culminando para uma maior investigações e aplicabilidade da lei vigente. A Convenção de Budapeste sobre o Crime Cibernético, é um tratado internacional assinado em 23 de novembro de 2001 e promulgado na Federação Brasileira em 12 de abril de 2023, visa o fortalecimento dos laços internacionais na cooperação no enfretamento dos crimes cometidos por meio da Internet e com a utilização de computados.

Casos emblemáticos e norteadores que envolvem a violação de dados pessoais e crimes financeiros como o da atriz Carolina Dieckmann, demonstram os desafios e obstáculos que enfrenta o Ordenamento Penal Brasileiro. As decisões jurídicas que abrangem a tal instituto tem se afirmado na importância da proteção de dados pessoais e a responsabilização das empresas e indivíduos envolvidos.

Sob essa perspectiva a presente produção acadêmica, buscará analisar por meio de perspectivas legislativas, doutrinárias, artigos científicos, como tem-se vislumbrado as dinâmicas da responsabilidade penal na esfera dos crimes cometidos na Internet.

Nota-se, que em razão das vicissitudes digitais devem ser acompanhadas os meios para garantia de acesso seguro, políticas de privacidade, e probidade virtual de ambientes no ciberespaço à pessoa idosa, como forma de efetivação participação na vida familiar, comunitária, política e cidadania.

Cumpre destacar, que a problemática inserida é palpitante, urgente e de necessário debate pela sociedade e comunidade acadêmica, haja vista que hoje o mundo globalizado caminha para um cenário de inversão da pirâmide etária, ou seja, os jovens de hoje serão as pessoas idosas do futuro, as quais precisam de apoio e auxílio de capacitações para convivência com o dinamismo do ciberespaço.

2. CRIMES COMETIDOS NA ERA DIGITAL E À RESPONSABILIDADE PENAL NA LEGISLAÇÃO BRASILEIRA.

Muito se tem discutido, recentemente, que os crimes da era digital têm possuído um número significativo ao longo dos anos, essa evolução da tecnologia proporciona uma grande variedade de utilizações por meio digital. A era da internet e dos dados propagados por este meio trouxe consigo inúmeras vantagens, facilitando a maneira como a comunicação, trabalho e interação à distância.

Muitos utilizam com sabedoria para atender suas necessidades e ampliar seu conhecimento, contudo, alguns usam para adquirir uma vantagem em cima de outras pessoas e promover o crime, agindo de má-fé com o próximo. Como todo acontecimento temos a parte favorável, acompanha também à desfavorável, que é os crimes cometidos em uso digital, pessoas individuais, empresas e até o governo tem lidado com os ataques cibernéticos.

Os crimes digitais apresentam uma abrangente gama de exercícios ilícitos realizados através de celulares e notebooks. Dentre os mais divulgados, coloca-se em ênfase as fraudes eletrônicas, as quais envolvem as atividades derivadas como phishing, onde os infratores obtêm informações pessoais e individuais, como senhas e números de cartão de crédito, obtidas através de e-mails falsos ou site fraudulentos.

Tal invasão dos dispositivos se origina como uma prática comum e de fácil traquejo, visto que os hackers invadem os aparelhos eletrônicos com o objetivo de instalar malware e realizar atividades ilícitas. A disseminação dos vírus é uma ameaça significativa, utilizado para contaminar e danificar o acesso não autorizado aos sistemas e dados.

Tornou-se uma discussão global, e a cada dia tem se tornado mais comum esse tipo de ação criminosa, visto que ação visa atingir as pessoas em vulnerabilidade e de fácil acesso nessa situação prejudicial, onde fica a medida cabível para punir esses autores que obtém informações de forma desonrosa e retiram a segurança social da sociedade. Informações confidenciais, dados importantes e também arquivos pessoais, podem ser comprometidos com uma certa facilidade, onde os crimes cometidos contra a honra, que possuem o intuito de caluniar, difamar e injuriar permeiam as dimensões da era digital, sendo praticados através de redes sociais e outros tipos de acesso online.

A responsabilidade penal na legislação brasileira prevê a punição para esses crimes cibernéticos, invasões nos dispositivos com o intuito de afetar a honra e integridade da pessoa, conforme se vislumbra pelo artigo 154-A do Decreto Lei n.º 2.848 de 07 de dezembro de 1940:

Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede

de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita*: (Redação dada pela Lei nº 14.155, de 2021)*

§ 1°. *Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput. (Incluído pela Lei nº 12.737, de 2012)*

§ 2º. *Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico. (Redação dada pela Lei nº 14.155, de 2021) (grifo nosso).*

Em questão da responsabilidade penal, a legislação brasileira tem de ser torno evoluída em tal combate que envolvem o universo digital. Dentre as principais normas, a lei n.º 12.737/2012, tipificou tal delito relacionado à invasão dos dispositivos informáticos. Além disso, o Marco Civil da Internet, denominada como lei n.º 12.965 promulgada em 23 de abril de 2015, tornou-se um marco legal e fundamental para a regulamentação da utilização da internet no Brasil, de extrema importância para a proteção dos dados e privacidade dos usuários.

Bem como, a Lei n.º 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD), entrou em vigor na Federação Brasileira em 25 de agosto de 2020, objetivando a proteção dos direitos fundamentais dos cidadãos em respeito ao armazenamento, uso, coleta e tratamento dos dados pessoais da sociedade. Sua aplicabilidade se deduz à todas as empresas e órgãos públicos que tratar dos dados pessoais e informações personalíssimas, independentemente do seu porte e ramo de atuação.

A era digital coloca átona diversos obstáculos e desafios decorrentes da segurança e a justiça, exigindo uma certa adaptação e renovação constante da legislação brasileira e dos combates aos crimes cibernéticos. O ordenamento jurídico deve ter uma atuação robusta e efetiva, a qual seja capacidade para criminal e responder rapidamente frente as novas ameaças e proteger os direitos pessoais e a segurança da sociedade brasileira na esfera digital.

3. ANÁLISE DA LEI N.º 12.737, PROMULGADA EM 2012 (LEI CAROLINA DIECKMANN).

A Lei n.º 12.737, conhecida popularmente como Lei Carolina Dieckmann, representa um marco significativo em relação aos combates e proteção de dados pessoais frente a

criminalização das condutas ilícitas advindas do ambiente digital. Tal dispositivo tornou uma resposta à grande repercussão midiática que envolveu a atriz Carolina Dieckmannn, a qual teve o vazamento, sem seu consentimento, de suas fotos pessoais na internet, colocando em evidencia a lacuna legislativa que existia no combate aos crimes cibernéticos.

Neste contexto, a lei, em seu conteúdo, tornou e tipificou os crimes informáticos e invasivos não autorizados que visam a obtenção de adulterar e/ou destruir dados e informações personalíssimas. Bem como, prever a criminalização de tais delitos varia entre três meses à dois anos de detenção.

Nota-se, que um ponto crucial é a necessidade da autorização para obter o acesso aos dados e informações pessoais contidas nos dispositivos informáticos. Tal invasão sem o consentimento tornou-se um crime, mesmo que não haja qualquer intenção de causar ou disseminação de dano ou vantagem, visto que tal previsão legal objetiva unicamente em resguardar a privacidade dos indivíduos e assegurar totalmente as informações pessoas que possam ser acessadas indevidamente.

Nesta visão jurídica, a Lei n.º 12.737/2012 se firma nos princípios constitucionais presente na proteção à privacidade e à intimidade, consolidados no artigo 5°, inciso X, da Constituição Federal de 1988:

> ***Art. 5.*** *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:*
>
> *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. (grifo nosso).***

Sob este prisma, o cenário jurídico atual ainda é propenso para a propagação dos crimes cibernéticos no Brasil. A promulgação da Lei Carolina Dieckmann exige certa estruturação rebuscada de fiscalização e um excelente sistema jurídico capacitado para combater as questões envolventes em tal delito.

4. OS OBSTÁCULOS E PERSPECTIVAS FUTURAS NO ORDENAMENTO JURÍDICO BRASILEIRO PERANTE OS CIBERCRIMES.

A ação criminosa advinda da esfera digital impõe um desafio constante e complexo

para o Ordenamento Jurídico Brasileiro, visto que exige uma constate adaptação e reformulação das leis e normas para que possam conseguir acompanhar a crescente evolução tecnológica e das formas de delitos digitais. Frente a este cenário, torna-se imperativo analisar as perspectivas enfrentadas pela Federação Brasileira no combate aos crimes cibernéticos, também a exploração das futuras repostas jurídicas a tais ameaças.

Um dos principais fatos é a natureza internacional dos cibercrimes. Tais criminosos que cometem tais infrações operam frequentemente sob a espera internacional, utilizando das redes fora da nacionalidade para pratica e perpetrar os ataques e dificultar a devida identificação e responsabilização.

Nota-se, que a capacidade de operar tecnicamente das autoridades competentes brasileiras para tal combate enfrenta certas e significativas limitações. As investigações de tais crimes requerem habilidade e expertise que nem sempre estão ao serviço das forças de segurança e dos órgãos de justiça.

Bem como, a legislação brasileira ainda apresenta incipiente e torna desatualizado comparado aos países europeus e desenvolvidos. Mesmo que o Brasil possua avanços significativos com a promulgação de diversas leis que criminalizam tais delitos, como as leis n.° 12.737/2012 (Lei Carolina Dieckmann) e a Lei n.º 13.709/2018 (Lei Geral de Proteção de Dados – LGPD), ainda há nuancias que dificultam a aplicabilidade eficaz das normas.

No que tange as futuras perspectivas, torna-se crucial que a Federação Brasileira revise e invista em um sistem jurídico efica e traga segurança social e digital de cibernetica, devendo ser integrado e atualizado. Apontando uma certa necessidade de um investimento continuo em equipamento de segurança e tecnologia, bem como a cooperação internacional que vise o enfretamento os cibercrimes.

5. CONCLUSÃO.

Concluindo, a atual Era Digital, abrangida pelos grandes avanços tecnológicos, trouxe em sua bainha diversos benefícios e impões desafios significativos, com ênfase à segurança dos dados e informações pessoais. A fácil disseminação e acesso à informação coloca em risco e o surgimento dos novos delitos, denominados como cibercrimes, os quais afetam os indivíduos, sociedades e governos.

Para o enfrentamento de tais desafios, torna-se essencial a promoção de politicas públicas que objetivam a educação digital e conscientização da segurança cibernética e sobre o uso correto da internet. A cooperação dos países internacionais deve ser fortalecida no

combate e investimentos e aprimoramento em tecnologia especializada são necessários e essências para a criação de um ambiente digital seguro e fortalecido.

Em suma, a eficácia da Lei Carolina Dieckmann e da legislação brasileira no combate aos cibercrimes depende do esforço mutuo e conjunto do governo e do setor privado. Apenas através de uma abordagem que vise integral e colaborar será possível o enfrentamento das ameaças emergente, proteção dos direitos personalíssimos e uma resposta jurídica robusta e eficaz que vise proteger a sociedade e o ambiente digital.

6. REFERÊNCIAS.

BRASIL. Constituição da República Federativa do Brasil de 1988. Diário Oficial da União. Poder Legislativo, Brasília, DF, 5 out. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em 01 jul. 2024.

BRASIL, Código penal (1940). 45. ed. São Paulo: Saraiva, OAB, 2018.

Lei Carolina Dieckmann. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm Acesso em 05 de jul de 2024.

BRASIL. Lei n.º 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei n.º 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018.

Nunes Sobrinho, J. R., & Grott, S. (2022). Os sujeitos ativos no cibercrime e a responsabilidade penal do ofensor. Revista Científica Multidisciplinar Do CEAP, 4(2). Recuperado de http://periodicos.ceap.br/index.php/rcmc/article/view/162