CENTRO UNIVERSITÁRIO VALE DO SALGADO (UNIVS)
CURSO DE BACHARELADO EM DIREITO

ARTUR ANTÔNIO TEIXEIRA DIÓGENES DE OLIVEIRA

CRIMES CIBERNÉTICOS: a efetividade do direito penal no combate a invasão dos dispositivos informáticos

ICÓ-CE
2025

ARTUR ANTÔNIO TEIXEIRA DIÓGENES DE OLIVEIRA

CRIMES CIBERNÉTICOS: a efetividade do direito penal no combate a invasão dos dispositivos informáticos

Artigo Científico apresentado ao curso de Bacharelado em Direito do Centro Universitário Vale do Salgado (UNIVS), como requisito para a obtenção de título em bacharel em Direito.

Orientador: Prof. Me. Yago Bruno Lima Vieira.

ICÓ-CE
2025

ARTUR ANTÔNIO TEIXEIRA DIÓGENES DE OLIVEIRA

CRIMES CIBERNÉTICOS: a efetividade do direito penal no combate à invasão dos dispositivos informáticos

Artigo Científico apresentado ao curso de Bacharelado em Direito do Centro Universitário Vale do Salgado (UNIVS), como requisito para a obtenção de título em bacharel em Direito.

Aprovado em: _____/_____/2025

FICHA DE AVALIAÇÃO

_____

Prof. Me. Yago Bruno Lima Vieira Santos
Centro Universitário Vale do Salgado
Orientador

_____

Prof. Me. Ricelho Fernandes De Andrade
Centro Universitário Vale do Salgado
1º Examinador

_____

Prof. Esp. Francisco Marlúcio Paz Lima Júnior
Centro Universitário Vale do Salgado
2º Examinador

LISTA DE SIGLAS E ABREVIATURAS

BBS	Bulletin Board System
CE	Ceará
CEP	Comitê de Ética em Pesquisa
CP	Código Penal
DNS	Domain Name System
HC	Habeas corpus
IA	Inteligência Artificial
IP	Internet Protocol
MG	Minas Gerais
MPF	Ministério Público Federal
PF	Polícia Federal
PL	Projeto de Lei
PR	Paraná
RS	Rio Grande do Sul
SP	São Paulo
STF	Supremo Tribunal Federal
TLD	Top-Level Domain
UNIVS	Centro Universitário Vale do Salgado
URL	Uniform Resource Locator

RESUMO

OLIVEIRA, A. A. T. D. **CRIMES CIBERNÉTICOS:** a efetividade do direito penal no combate à invasão dos dispositivos informáticos. 2024. 22 f. Artigo Científico (Graduação em Direito) – Centro Universitário Vale do Salgado, Icó, 2024.

O presente estudo tem como objetivo avaliar a eficácia da Lei nº 12.737/2012 no combate aos crimes de invasão de dispositivos informáticos no Brasil. A pesquisa busca contextualizar a evolução dos crimes cibernéticos e analisar como essas condutas vêm sendo regulamentadas no país, com ênfase na resposta da legislação penal, especialmente da mencionada norma, às demandas da era digital. O objetivo geral é examinar a aplicação da referida lei nos casos de violação a dispositivos informáticos, evidenciando os mecanismos de responsabilização dos infratores e seus efeitos jurídicos. Como objetivos específicos, propõe-se: (i) contextualizar a evolução histórica dos crimes cibernéticos e sua regulamentação no Brasil; (ii) examinar a legislação penal vigente sobre invasões cibernéticas, com foco na Lei nº 12.737/2012; e (iii) discutir seus efeitos práticos e as principais críticas que lhe são atribuídas. A problemática central parte do seguinte questionamento: como o ordenamento jurídico brasileiro tem aplicado a Lei Carolina Dieckmann no combate aos cibercrimes, especialmente em relação à invasão de dispositivos e à violação de dados confidenciais, e quais são os desafios enfrentados em sua efetiva implementação? A análise justifica-se pela relevância da Lei nº 12.737/2012 como marco legislativo no enfrentamento dos crimes digitais, ainda que tenha deixado lacunas. A posterior promulgação da Lei nº 14.155/2021 buscou suprir parte dessas falhas, ampliando a criminalização das condutas e agravando as sanções. A pesquisa utiliza o método bibliográfico, com base em livros, artigos, legislações e doutrinas jurídicas, propondo uma reflexão crítica sobre o aprimoramento da legislação penal frente às novas formas de criminalidade digital.

Palavras-Chave: Crimes cibernéticos. Invasão de dispositivos informáticos. Lei Carolina Dieckmann.

ABSTRACT

OLIVEIRA, A. A. T. D. **CYBER CRIMES:** the effectiveness of criminal law in combating the invasion of computer devices. 2024. 22 f. Scientific Article (Graduation in Law) – Vale do Salgado University Center, Icó, 2024.

This study aims to evaluate the effectiveness of Law No. 12,737/2012 in combating computer hacking crimes in Brazil. The research seeks to contextualize the evolution of cybercrimes and analyze how these behaviors have been regulated in the country, with an emphasis on the response of criminal legislation, especially the aforementioned law, to the demands of the digital age. The general objective is to examine the application of the aforementioned law in cases of hacking of computer devices, highlighting the mechanisms for holding offenders accountable and their legal effects. The specific objectives are: (i) to contextualize the historical evolution of cybercrimes and their regulation in Brazil; (ii) to examine the current criminal legislation on cyber hacking, focusing on Law No. 12,737/2012; and (iii) to discuss its practical effects and the main criticisms attributed to it. The central issue is based on the following question: how has the Brazilian legal system applied the Carolina Dieckmann Law to combat cybercrimes, especially in relation to the invasion of devices and the violation of confidential data, and what are the challenges faced in its effective implementation? The analysis is justified by the relevance of Law No. 12,737/2012 as a legislative framework in combating digital crimes, even though it left gaps. The subsequent enactment of Law No. 14,155/2021 sought to fill some of these gaps, expanding the criminalization of conduct and increasing sanctions. The research uses the bibliographic method, based on books, articles, legislation and legal doctrines, proposing a critical reflection on the improvement of criminal legislation in the face of new forms of digital crime.

Keywords: Cyber crimes. Criminal law. Hacking of computer devices. Carolina Dieckmann Law. Brazilian legislation.

SUMÁRIO

1 INTRODUÇÃO

A Informática é um campo das ciências da informação e computação, voltado ao estudo dos processos de coleta, armazenamento, processamento, transferência e disseminação de dados digitais. O termo deriva da soma de "informação" e "automática", representando, resumidamente, o processo de tratamento automatizado da informação.

Atualmente, com a crescente adoção de interfaces e sistemas totalmente informatizados, o conhecimento de informática é cada vez mais necessário para que os indivíduos alcancem autonomia tecnológica. Nestes casos, os principais objetivos de informatização e automatização, são agilizar os serviços e reduzir a ocorrência de erros humanos.

Com o avanço tecnológico surge novas modalidades de atos ilícitos, assim, observou-se a necessidade da criação de normas protetoras aos afetados por estes atos. Ao longo dos anos, à medida que a Internet e suas formas se expandiam, o número de malwares aumentou, tornando-os uma ferramenta extremamente útil para que os hackers obtenham acesso a outros computadores e invadam redes para realizar ataques cibernéticos.

Esta pesquisa justifica-se pela relevância de analisar a legislação penal relacionada aos crimes informáticos, especialmente quanto à responsabilização dos infratores e à efetividade das penalidades. Considerando o avanço tecnológico, é fundamental atualizar o arcabouço jurídico, identificar lacunas e sugerir melhorias. A análise de casos práticos, aliada à cooperação internacional, é essencial para enfrentar a dimensão transnacional dos cibercrimes e assegurar a segurança digital.

O presente estudo tem como objetivo geral a análise da aplicação da Lei 12.737/2012 (Lei Carolina Dieckmann) nos casos de violação aos dispositivos informáticos, demonstrando os tipos de mecanismos para a responsabilização dos infratores previstos nesta lei e seus efeitos legais e traz os seguintes objetivos específicos: contextualizar a evolução histórica dos crimes cibernéticos e como eles são regulamentados no Brasil, examinar a legislação penal em vigência no Brasil referente aos crimes de invasão cibernética, especificamente a Lei nº. 12.737/2012 (Lei de Carolina Dieckmann) e discutir os efeitos e critícas referentes a esta lei.

A problemática central da pesquisa busca analisar a aplicação do sistema jurídico brasileiro no combate aos cibercrimes, considerando tanto as decisões judiciais quanto as perspectivas doutrinárias. O estudo investiga o impacto da Lei 12.737/2012 (Lei Carolina Dieckmann) na repressão e punição dos crimes relacionados à invasão de dispositivos e à violação de dados confidenciais no Brasil, examinando sua efetividade na prática e os desafios enfrentados na sua implementação.

Esta análise foi realizada por meio de pesquisa bibliográfica, com estudos de livros, artigos, legislações e jurisprudências, com o objetivo de solucionar os problemas apresentados. Além disso, adota uma abordagem aplicada, focada na identificação de problemas e na proposição de soluções na área dos cibercrimes, elaborando diagnósticos e análises práticas para atender demandas de atores sociais ou instituições, conforme Thiollent (2009). A pesquisa também tem caráter exploratório, buscando aproximar o pesquisador do problema central e esclarecer a temática. De acordo com Gil (1991), a pesquisa exploratória, especialmente a bibliográfica, auxilia na construção de hipóteses e oferece base teórica para reflexão e crítica sobre o tema.

O primeiro capítulo abordará a evolução histórica dos crimes informáticos, suas principais técnicas e condutas, além da relação entre informática e Direito Penal, detalhando a classificação desses crimes. Também destacará o papel da tecnologia na sociedade, evidenciando sua contribuição para o acesso ágil à informação, eficiência processual, globalização do conhecimento e redução da alienação política, demonstrando que seu impacto vai além do desenvolvimento de softwares. Para Nicholas Carr (apud. Gerschenfeld, 2010, p. 2), a Internet está mudando a nossa forma de pensar. Estamos terceirizando nossa memória e nossa identidade.

Em suma, o último capítulo trará a perspectiva do Cibercrime junto aos tribunais. Estarão presentes casos levados aos tribunais, buscando exemplificá-los e ilustrá-los.

Como resultados pretendidos, espera-se identificar lacunas na legislação vigente e propor reflexões sobre a eficácia das normas atuais na responsabilização penal de infratores virtuais, contribuindo para o aprimoramento do combate aos crimes cibernéticos.

O tema abordado é de inegável relevância social, pois além de examinar questões jurídicas, evidencia práticas comuns desta efêmera modalidade, com o qual o Direito Penal busca acompanhar e pugnar habitualmente.

Portanto, deseja-se que, ao folhear esse trabalho, o examinador aprofunde-se e se identifique com o assunto extremamente útil e atual que será abordado. Ademais, que os juristas se especializem neste ramo, para agregar ainda mais à legislação e à defesa dos acometidos pelos delitos advindos dos crimes cibernéticos.

2 REFERENCIAL TEÓRICO

O capítulo apresenta um panorama histórico dos crimes cibernéticos, destacando sua evolução e os impactos do avanço tecnológico. Também discute a resposta do ordenamento jurídico brasileiro a esses delitos, enfatizando a necessidade de regulamentações específicas para lidar com as novas formas de criminalidade digital. Nos capítulos seguintes, será analisada a evolução da legislação penal brasileira em relação aos crimes cibernéticos, incluindo as melhorias trazidas pelas leis, suas lacunas e controvérsias, como a definição imprecisa de "invasão". Além disso, será abordada a necessidade de atualização constante da legislação para enfrentar a evolução dos crimes digitais, destacando os desafios e sugerindo avanços para tornar o combate a esses crimes mais eficaz. A divisão dos tópicos foi feita com base na instrumentalidade dos temas. Primeiro, é necessário contextualizar o objeto do estudo, para então abordar seu conteúdo de forma clara.

2.1 CONTEXTUALIZAÇÃO DOS CRIMES CIBERNÉTICOS E A IMPRESCRITIBILIDADE DA REGULAMENTAÇÃO NO BRASIL

Na França, em meados de 1820, Joseph-Marie Jacquard criou uma máquina de tear automatizada, com capacidade de repetir várias ações, anteriormente realizadas manualmente na produção de tecidos específicos. Com essa inovação, surgiu um temor entre os trabalhadores que, logo se preocuparam com a possibilidade da perda de seus empregos, levando-os à de sabotagem a fim de enfraquecer a utilização da nova tecnologia que vira a emergir (Jesus; Milagre, 2016).

Em 1939, o Serviço de Inteligência Americano escalou Alan Turing para investigar o sigilo das máquinas codificadoras eletromagnéticas. Neste período, o rompimento de técnicas procedimentais e códigos para proteção e ocultação de informações já eram fragmentados (Jesus; Milagre, 2016).

O início da era computacional moderna inicia-se com Charles Babbage, onde há uma busca da linguagem universal e o romantismo numérico. Mundialmente, a literatura internacional informa que os crimes informáticos se iniciaram em 1960, onde foram encontrados os primeiros estudos sobre a temática, sendo delatados infrações de alterações, sabotagens de sistemas operacionais e cópias. Em 1970, já era mencionado o termo *hacker.* Em 1979, Daniel Bell cita o termo *sociedade da informação*. “A informação é necessária para organizar e fazer funcionar tudo, desde a célula até a General Motors” (Bell, 1979, p. 169).

No Brasil, foi em 1999 que noticiaram os primeiros delitos de de *phishing scam* bancário (apropriação de senhas). Vale mencionar, que a essa época um empresário varejista enviou um e-mail ao mercado financeiro de Londres, informando fake News sobre a quebra de um banco. Desde então, houve diversas divergências acerca desses crimes, restando evidenciado que tais delitos podem ser executados em qualquer parte do globo, bem como a dificuldade de efetuar uma investigação nesses casos. Daí então, iniciou-se uma reflexão diante da necessidade de criação de leis que tratassem dos crimes cibernéticos. Wendt e Nogueira abordam que:

> Em virtude da constante evolução tecnológica que acompanhamos, principalmente com a inclusão, cada dia mais, de dispositivos que acessam a rede mundial de computadores, os crimes cibernéticos têm acompanhado esse ritmo e, diariamente, tem sido observado o surgimento de novas ameaças (Wendt; Nogueira, 2020; p.242).

O primeiro crime cibernético ocorreu em 1997, foi uma ameaça de cunho sexual atribuída a um jornalista por meio de e-mails. A polícia descobriu o autor das mensagens e ele foi obrigado a efetuar cursos para a Academia de Polícia Civil (Dullius; Hippler; Franco, 2012, p. 3).

Em 1998, no histórico julgado do HC 76.689/PB, o qual teve como relator o Ministro Sepúlveda Pertence, o STF já discutia um caso envolvendo a pornografia infantil nas BBS (*Bulleting Board System/Internet).* Neste ínterim, o ministro explicou que não é obrigatório a criação de uma lei específica para responder os delitos cibernéticos, pois a tecnologia é apenas um novo meio a ser utilizado para a prática de delitos já tipificados. Como:

Em 1998, em julgado que se tornou histórico, no HC 76.689/PB, relatado pelo Ministro Sepúlveda Pertence, o Supremo Tribunal Federal já enfrentava um caso envolvendo pornografia infantil nas antigas BBS (*Bulleting Board System/Internet*). À época, poderia alguém já imaginar que haveria necessidade de lei específica para responder a tais delitos. Mas não! O Ministro deu aula ao explicar que nem todos os delitos cibernéticos necessitavam de nova tipificação, eis que em muitos a tecnologia era só um novo meio utilizado para concretização de delitos conhecidos. "A mesma Polícia Federal já afirmou que o crime informático gera mais dinheiro que o narcotráfico. Dados do CNB – Colégio Notarial do Brasil – indicam que o número de crimes virtuais no país aumentou 70% entre 2012 e 2013" (Kurtz, 2014, p. 1).

O Direito é o conhecedor capaz de proteger os lesados, aplicando as normas jurídicas vigentes, como também, criando tipificações específicas, impossibilitando a "analogia *in malam partem*" e ao passo que surgem novos bens jurídicos na sociedade, o Direito tem como dever primordial proteger esses bens (Jesus; Milagre, 2016).

2.2 LEGISLAÇÃO PENAL BRASILEIRA APLICADA AOS CRIMES CIBERNÉTICOS

Há importante esclarecimento sobre a viabilidade do enquadramento de algumas atividades que causam danos aos usuários de aparelhos digitais. Porém, existem situações que não existem previsões penais para adequar perfeitamente os delitos, tendo isto por base, foi proposto o Projeto de Lei nº 84/1999 pelo ex-deputado Luiz Piauhylino, visando proporcionar melhores argumentos para responsabilização de crimes cibernéticos.

Este projeto foi aprovado na Câmara Federal no ano de 2003, posteriormente tramitou no Senado, e somente em 2008 ele foi aprovado definitivamente, porém com uma substituição em sua nomenclatura (Projeto de Lei nº 89/2003). Depois o projeto de lei retornou para a Câmara Federal, e no final de 2012, foi aprovado. O referido projeto foi sancionado no dia 30 de novembro de 2012 (Lei nº 12.735/12), comumente conhecida como Lei Azeredo. Essa lei tipifica infrações cometidas pelos meios eletrônicos ou similares, contra sistemas informatizados. A lei modifica o Código Penal, o Código Penal Militar e a Lei de Combate ao Racismo, incluindo um artigo que submete a retirada imediata de mensagens racistas da rede. Além disso, essa lei institui delegacias especializadas à investigação e combate dos crimes informáticos, como as Polícias Civis e Federais, que deverão criar setores e equipes especiais para conter ações delituosas. No entanto, apesar dos avanços proporcionados pela Lei Azeredo na tipificação de crimes cibernéticos e na criação de delegacias especializadas, sua efetividade ainda é alvo de debates, pois a rápida evolução da tecnologia exige atualizações constantes na legislação para acompanhar as novas formas de criminalidade digital. Além disso, a aplicação da lei depende da capacitação das autoridades e da integração com outras normativas, como o Marco Civil da Internet e a Lei Carolina Dieckmann, para garantir uma abordagem mais eficaz no combate aos crimes informáticos no Brasil.

Nesse contexto:

> Necessariamente, no Brasil ainda não foi e deverá ser traçado um planejamento e uma preparação para todos os problemas gerais relacionados com o tema, existentes e os que ainda surgirão, especialmente a reestruturação do sistema policial voltado à cibe investigação (Wendt; Nogueira, 2020, p. 242).

Em 16 de maio de 2012, em resposta ao escândalo gerado pela divulgação das fotos da atriz Carolina Dieckmann, o plenário da Câmara dos Deputados aprovou o projeto de lei do deputado Paulo Teixeira, que define especialmente o crime de invasão de dispositivos eletrônicos. O PL 2793/2011 foi enviado para a apreciação do Senado e, unido com uma parte

do “projeto Azeredo”, que também recebeu aprovação. Em 30 de novembro de 2012, a Lei nº 12.737 foi sancionada, sendo popularmente conhecida como Lei Carolina Dieckmann.

A referida lei inseriu ao código penal o delito de invasão de dispositivos informáticos.

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita (Código Penal, 2021).

A Lei Carolina Dieckmann foi criada após um ocorrido com a atriz global, que teve suas fotos íntimas vazadas em 2011. Hackers adentraram seu computador através do e-mail dela e antes de vazarem as imagens, eles tentaram colher quantias como forma de chantagem para que as fotos não fossem divulgadas. Foi daí que surgiu a primeira lei com o objetivo de proteger dados e informações no âmbito digital.

A Lei dispõe sobre algumas condutas que são punidas, como o ato de violar um dispositivo particular com intuito de adulteração, obter ou destruir informações e dados sem autorização do titular destes. Também a Lei dispõe que o ato de instalar vírus (invasão) computadores não se trata de atos preparatórios, mas sim, um crime cibernético.

Ademais, a Lei Carolina Dieckmann também define que é considerado crime a divulgação do conteúdo colhido ilegalmente sem autorização do titular daquela informação, a fim de obter benefício financeiro próprio ou para outrem.

Em dezembro de 2022 a lei mencionada completou 10 anos, contudo ainda carece de atualizações, buscando a melhoria das normas para adequar-se cada vez mais aos casos que, ao passar do tempo só crescem e sofrem mutações, como também eliminar ambiguidades do texto da norma.

Apesar da lei ter uma eficácia positiva, também há consequências negativas. Especialistas criticam o fato da moderação de suas punições e por apenas criminalizar o acesso de dados caso um obstáculo seja violado. Ou seja, significa que se alguém acessar dados de um dispositivo gratuito, como um aparelho celular desbloqueado, não será tipificado como crime (Nascimento, 2016). Assim, não basta apenas a garantia da execução da lei, mas é preciso que os usuários protejam seus dispositivos com antivírus, senhas e outros meios seguros para evitar invasões.

O advogado criminalista Luiz Augusto Sartori de Castro argumenta: “ausência de definição de diversos termos técnicos inseridos na lei, o que também inviabiliza a aplicação do tipo penal comentado”, como exemplo trata sobre o Art.154-A, CP, que aborda a invasão de

sistemas informáticos, “vê-se que faltou suporte técnico-jurídico aos legisladores na redação dos dispositivos”, “Quando a discussão chegar ao Poder Judiciário, deixará de ser punida a grande parcela daqueles que acessam indevidamente sistemas de informática. Isso porque não o fazem à força, como exige o tipo penal ao se valer do verbo invadir” (Castro apud., Sá, 2021). Para a ocorrência do crime é necessário a violação de um mecanismo de segurança, porém, não ficou claro por parte da lei quais tipos de mecanismos são esses.

> Diante de tantas lacunas, a lei apesar da sua importância, não consegue amparar boa parte da sociedade, pois umas parcelas de indivíduos são leigas em relação a dispositivos de segurança ou até mesmo não possuem recursos suficientes para arcar com a instalação de programas, como antivírus ou quaisquer outros que sirvam como forma de proteção pessoal dos seus dados (Sá, 2021, p. 11).

O fato da atribuição de penas brandas há quem pratica delitos cibernéticos é uma crítica ao sistema judiciário brasileiro, visto que, encoraja ações de futuros infratores, tendo em vista que, os prejuízos dos lesados podem ser bastante significativos, além disso, por esses crimes possuírem penas mínimas, caso o julgamento dos casos não seja hábil, corre o risco de haver a prescrição, assim, não havendo a punição, a qual é indispensável.

Posto isso, exige-se o estabelecimento de leis mais concretas, buscando a garantir recursos suficientes para a investigação, a defesa da cooperação internacional e a educação dos usuários digitais acerca da segurança digital e o reconhecimento da atividade criminosa. A Lei Carolina Dieckmann representa uma iniciativa relevante na discussão sobre crimes cibernéticos, embora sua eficácia enfrente desafios devido às constantes mudanças nesse tipo de crime (Nascimento, 2016).

> Assim, espera-se que, com a Lei nº 12.735/12, possam os órgãos policiais se adequar às exigências sociais de investigação eficaz dos crimes cibernéticos, especialmente em razão da pulverização da Internet e uso cada vez maior, principalmente o provocado pela pandemia do coronavírus. A instalação de delegacias e/ou laboratórios de inteligência cibernética nos estados é fundamental para o atendimento a essa demanda (Wendt; Nogueira, 2020, p. 249).

A Lei n. 12.737/2012 é uma iniciativa governamental importante, porém está a distantes passos de solucionar todos os problemas referentes ao crime cibernético no Brasil. A solução do problema não de fácil resolução e com certeza não será resolvida apenas com a edição de leis. É preciso ir além, dispondo educação digital nas escolas e estabelecimentos educacionais, políticas criminais e uma preparada estrutura investigativa.

2.3 OS EFEITOS E CONTROVÉRSIAS DA LEI CAROLINA DIECKMANN

Antes da vigência da Lei 12.737/2012 (Lei Carolina Dieckmann), estudiosos da área de direito informático tratavam que, 95% das condutas ilícitas realizadas no ambiente digital já encontrava previsão em outras normas penais. Crimes como estelionato, injúria, calúnia, difamação e até invasão de sistemas podiam ser enquadrados em legislações gerais, mesmo que estas não fossem originalmente elaboradas para tratar de crimes cibernéticos, os 5% restantes tratam-se de condutas do ambiente digital que ainda não estão previstas na lei (Penido, 2013).

A Lei 12.737/2012 foi criada com o propósito de suprir as lacunas existentes e ajustar o ordenamento jurídico às novas demandas trazidas pela evolução tecnológica. Essa legislação trouxe maior clareza e especificidade para o tratamento dos crimes informáticos, reduzindo significativamente o pequeno percentual de condutas não contempladas e tornando a repressão aos crimes cibernéticos mais eficaz e assertiva. A lei visa punir condutas criminosas praticadas pelos meios informáticos, prevê a pena de detenção, de 3 meses a 1 ano, e multa, bem como concede vantagens aos crimes de menor potencial ofensivo. Os infratores não se intimidaram com a disposição legal, ou seja, o objetivo da sanção não fora alcançado com bom desempenho (Beretta, 2014).

A análise do termo “invasão” referente a dispositivos informáticos levanta questões significativas no âmbito jurídico. Oliveira (2013) propõe uma reflexão essencial: o uso do computador de outra pessoa sem permissão configura uma invasão? Essa indagação ressalta a importância de considerar as circunstâncias e as intenções por trás do acesso não autorizado. Dependendo do contexto, tal ação pode ser interpretada como uma violação da privacidade digital, especialmente quando há a intenção de acessar informações confidenciais ou causar danos. No entanto, a interpretação legal pode variar conforme a avaliação específica de cada caso e a aplicação das legislações vigentes.

> Se houver violação indevida de mecanismo de segurança, como a senha, por exemplo, pode-se dizer que sim, mas se a pretensa vítima esqueceu o computador ligado a resposta será negativa. De todo modo, o tipo penal me parece um pouco genérico. Somente haverá crime em caso de invasão de dispositivo (computador, periféricos, etc.). Se o autor se limitar a invadir um perfil de rede social, um e-mail, banco de dados ou um álbum de fotografias, sem passar pelo computador da vítima, não incidirá no crime em análise. Cuida-se de um erro crasso do legislador (Oliveira, 2013).

Ou seja, não há uma invasão direta no equipamento informático do usuário, os dados são acessados a partir de redes sociais, e-mails e serviços de armazenamento em nuvem, que oferecem aos usuários a possibilidade de guardar suas informações em ambientes virtuais, como

Facebook, Instagram, Google Drive, Dropbox, iCloud, entre outros. Essas ferramentas permitem que os usuários armazenem seus dados em servidores virtuais, ao invés de mantê-los exclusivamente em seus dispositivos físicos. Portanto, mesmo sem invadir o equipamento em si, é possível acessar e roubar informações diretamente desses ambientes digitais, o que configura um tipo de crime cibernético.

A Lei Carolina Dieckmann gera diversos debates, sendo um dos principais a sua redação vaga e a falta de aspectos técnicos precisos. Um exemplo disso é a dúvida sobre a criminalização da invasão de um dispositivo próprio, visto que, o Art. 154-A, trouxe o crime denominado "Invasão de dispositivo informático", trata-se da invasão de qualquer dispositivo informático alheio, o que pode resultar em diversas interpretações por parte dos profissionais da área jurídica, gerando, assim, incertezas nas decisões judiciais.

Outro ponto controverso é a ausência de definição quanto ao tipo de dispositivo em que o crime pode ocorrer, o que deixa espaço para interpretações variadas por parte do Judiciário e do Ministério Público.

A redação original da lei de 2012 estabelecia que o crime de invasão de dispositivo informático era o "acesso de forma não autorizada de dispositivo informático alheio, conectado ou não a uma rede de computadores, através da violação de mecanismos de segurança, com a intenção de obter, modificar ou excluir dados ou informações sem o consentimento expresso ou implícito do proprietário do dispositivo, ou ainda, instalar falhas para obter benefícios ilegais". Com a Lei 14.155/2021, que aumentou a pena, houve uma mudança significativa: foi removido o trecho que mencionava a violação de mecanismo de segurança. Dessa forma, tornou-se possível cometer o crime de violação de dispositivo informático sem a necessidade de infringir um mecanismo de proteção. O trecho removido da lei servia como um critério, limitando a punição apenas a atos que envolvessem sistemas ou estruturas protegidos ativamente. Com essa alteração, o cenário mudou. Agora, se uma empresa expuser dados que deveriam estar protegidos mesmo que seja por erro, a "obtenção, adulteração ou destruição" desses dados sem autorização será punida, algo que antes não era possível, pois a falta de um mecanismo de segurança impedia a caracterização do crime. O tipo penal, portanto, foi alterado: o simples acesso não autorizado, sem a necessidade de violação de segurança, pode ser agora considerado crime. Em outras palavras, basta que o responsável não permita o acesso aos dados, e que haja a intenção de obter, modificar ou destruir essas informações, para que a conduta seja classificada como criminosa.

O requisito da autorização ainda se mantém. Caso alguém acesse dados públicos e os obtenha sem a devida permissão (ou altere ou destrua esses dados), pode ser punido, pelo menos

em teoria. Se o autor tiver a intenção de prejudicar a empresa ou outras pessoas, a lei deve alcançar seu objetivo. No entanto, há o risco de abuso na aplicação dessa norma. Esse é o problema de tipos penais excessivamente amplos, que podem afetar o princípio da taxatividade na legislação penal. A sociedade deve ser protegida contra leis penais imprecisas, vagas ou ambíguas. O risco de injustiças é evidente.

Embora a Lei Carolina Dieckmann tenha sido um passo importante para a proteção dos dados pessoais contra crimes virtuais, ainda é possível perceber que a legislação precisa ser aprimorada para eliminar ambiguidades e garantir uma interpretação mais clara e objetiva.

Dado o exposto, é possível analisar os dados presentes nos demais relatórios anuais abaixo, para mensurar a ocorrência de crimes cibernéticos, denúncias e estatísticas sobre o reconhecimento de DNS maliciosos, esses servidores são responsáveis por fornecer respostas incorretas para nomes de domínio de instituições vítimas, geralmente instituições financeiras, plataformas de comércio eletrônico, redes sociais ou domínios amplamente reconhecidos.

2.3.1 Relatórios sobre crimes cibernéticos no Brasil

RELATÓRIO SOBRE CRIMES CIBERNÉTICOS NO BRASIL – JANEIRO A DEZEMBRO DE 2024

O presente relatório apresenta uma análise dos dados sobre crimes cibernéticos ocorridos no Brasil ao longo do ano de 2024. O levantamento foi feito pela Polícia Federal e abrange um total de 311 registros distribuídos entre 28 estados monitorados, classificando os delitos conforme sua natureza e detalhando as principais ações realizadas pelas autoridades competentes.

1. Estatísticas Gerais

No período analisado, foram contabilizados:

- **386** prisões em flagrante;
- **1.063** operações realizadas;
- **92** vítimas resgatadas em casos de abuso sexual infantojuvenil;
- **1.457** mandados de busca e apreensão cumpridos.

2. Estados com Maior Incidência de Crimes Cibernéticos

Os estados que registraram o maior número de ocorrências foram:

1. **São Paulo (SP)** – 19 registros;
2. **Paraná (PR)** – 17 registros;
3. **Ceará (CE)** – 17 registros;
4. **Minas Gerais (MG)** – 16 registros;
5. **Rio Grande do Sul (RS)** – 15 registros.

3. Principais Tipos de Crimes Cibernéticos

Os crimes registrados foram categorizados em cinco áreas de atribuição:

- **Crimes cibernéticos relacionados ao abuso sexual infantojuvenil**: 251 casos, representando a maior parcela dos registros.
- **Fraudes bancárias eletrônicas**: 38 ocorrências.
- **Crimes de alta tecnologia**: 14 registros.
- **Crimes cibernéticos classificados como "legado"**: 6 casos.
- **Crimes cibernéticos de ódio**: 2 ocorrências.

Os dados evidenciam que a maior parte das ações esteve relacionada a crimes de abuso sexual infantojuvenil, demonstrando a necessidade de reforço contínuo nas políticas de combate a esse tipo de delito. Além disso, fraudes bancárias eletrônicas também se destacam como um problema relevante no cenário da segurança cibernética.

O relatório da SaferNet constatou que no ano de 2024, a Central de Denúncias recebeu e processou 100.077 denúncias anônimas envolvendo 68.286 páginas (URLs) distintas (das quais 41.192 foram removidas até aqui) escritas em 9 idiomas e hospedadas em 10.138 domínios diferentes, de 209 diferentes TLDs e conectados à Internet através de 10.628 números IPs distintos, atribuídos para 71 países em 6 continentes. As denúncias foram registradas pela população através dos 2 hotlines brasileiros que integram a Central Nacional de Denúncias de Crimes Cibernéticos, do Ministério da Justiça.

Já a Cert.br em seu relatório, contém estatísticas sobre servidores DNS maliciosos, monitorados pelo CERT.br, cobrindo o período de 1º de janeiro de 2024 a 29 de março de 2025.

Os dados apresentam a quantidade de servidores DNS ativos diariamente, diferenciando aqueles localizados no Brasil e no exterior. O relatório é visualizado por meio de gráficos que mostram a evolução desses servidores ao longo do tempo, tendo em 19 de setembro de 2024 o pico das atividades desses servidores maliciosos.

Um servidor DNS malicioso está diretamente relacionado aos crimes cibernéticos, pois pode ser utilizado em ataques como phishing, redirecionamento malicioso (DNS spoofing) e man-in-the-middle, levando as vítimas a sites falsos que imitam páginas legítimas de instituições financeiras, comércio eletrônico e redes sociais. Esses ataques visam roubar credenciais, informações bancárias e outros dados sensíveis. Além disso, essa prática pode configurar crimes previstos na legislação brasileira, como invasão de dispositivo informático (Lei 12.737/2012 - Lei Carolina Dieckmann) e estelionato eletrônico (art. 171, §2º-A do Código Penal).

3 CONSIDERAÇÕES FINAIS

Este estudo examinou a relação entre o Direito e o ambiente digital, especialmente no que diz respeito às condutas ilícitas praticadas na internet, aos mecanismos de repressão dessas ações e, por conseguinte, à resposta da legislação brasileira frente aos crimes cibernéticos. Além disso, analisou os impactos e desdobramentos dessas infrações no contexto jurídico e social. A pesquisa evidenciou a relevância do Direito Penal no enfrentamento dos crimes informáticos e, ainda, destacou sua influência na formação e atuação dos profissionais da área, ressaltando, portanto, a necessidade de um entendimento aprofundado sobre o tema para uma aplicação mais eficiente da legislação.

No decorrer da investigação, foram abordados os principais dispositivos legais que regulamentam os crimes cibernéticos, bem como decisões judiciais e dados estatísticos que refletem a evolução dessa modalidade criminosa. Os resultados indicam que, apesar da força normativa das leis vigentes, ainda assim há necessidade de revisões e aprimoramentos que garantam maior eficácia. Dessa forma, o cenário analisado ressalta a importância de atualizações legislativas contínuas, bem como de uma maior articulação entre os órgãos de segurança e, igualmente, do fortalecimento da cooperação internacional, com vistas a combater essas infrações de maneira mais eficiente.

Assim, este estudo contribui para a ampliação do debate sobre os cibercrimes, fornecendo subsídios para pesquisas futuras e para o aperfeiçoamento das políticas e práticas voltadas à segurança digital. Sugere-se, ainda, que novas investigações sejam conduzidas para avaliar o impacto das recentes mudanças legislativas e a efetividade de propostas normativas emergentes, como o Projeto de Lei de Proteção de Dados e Segurança Cibernética. Por fim, destaca-se que a capacitação contínua dos profissionais do setor jurídico e da segurança digital pode ser um fator determinante para o fortalecimento da proteção cibernética no Brasil. Logo, a continuidade das pesquisas nessa área revela-se essencial para assegurar os direitos digitais e, consequentemente, promover um ambiente virtual mais seguro, regulado e democrático para toda a sociedade.

REFERÊNCIAS

AGÊNCIA SENADO. Marco Civil da Internet completa dez anos ante desafios sobre redes sociais e IA. **SENADO FEDERAL**. Disponível em: https://www12.senado.leg.br/noticias/materias/2024/04/26/marco-civil-da-internet-completa-dez-anos-ante-desafios-sobre-redes-sociais-e-ia. Acesso em: 25 out. 2024.

BRASIL. Ministério Público Federal. Câmara de Coordenação e Revisão, 2ª. **Crimes Cibernéticos:** Coletânea de Artigos. Brasília: MPF, 2018. Volume 3. Disponível em: http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes. Acesso em: 14 out. 2024.

BRASIL. Polícia Federal. Diretoria de Combate a Crimes Cibernéticos. Dados de crimes cibernéticos: janeiro a dezembro de 2024 (parcial). Brasília, 2025. Disponível em: https://www.gov.br/pf/pt-br/acesso-a-informacao/estatisticas/diretoria-de-combate-a-crimes-ciberneticos-dciber/dados-de-crimes-ciberneticos-janeiro-a-dezembro-de-2024-parcial/view. Acesso em: 1 abr. 2025.

CERT.BR. **Estatísticas sobre DNS malicioso**. Disponível em: https://stats.cert.br/dns-malicioso/. Acesso em: 1 abr. 2025.

DIO. **O que é a biblioteca Random, um hash e multithreading?**. Disponível em: https://www.dio.me/articles/o-que-e-a-biblioteca-random-um-hash-e-multithreading. Acesso em: 14 out. 2024.

EMAG – Escola de Magistrados da Justiça Federal da 3ª Região. **Investigação e prova nos crimes cibernéticos**. São Paulo: Tribunal Regional Federal da 3ª Região, 2017.

FACHINI, T. Lei Carolina Dieckmann: tudo o que você precisa saber sobre. 2023. **PROJURIS**. Disponível em: https://www.projuris.com.br/blog/lei-carolina-dieckman-tudo-o-que-voce-precisa-saber-sobre/. Acesso em: 20 out. 2024.

FMP. **Lei Carolina Dieckmann: você sabe o que essa lei representa?** Disponível em: https://fmp.edu.br/lei-carolina-dieckmann-voce-sabe-o-que-essa-lei-representa/#:~:text=Quais%20s%C3%A3o%20as%20cr%C3%ADticas%20que,e%20carecer%20de%20aspectos%20t%C3%A9cnicos. Acesso em: 16 nov. 2024.

FREITAS, R. D. **Dicionário sobre crimes cibernéticos:** crimes e fraudes cibernéticas para advogados e funcionários do poder judiciário – descomplicando. V.1. Fevereiro de 2024.

IRIS, B. H. **Punição de crimes cibernéticos em 2021:** efeitos das alterações na Lei Carolina Dieckmann. Disponível em: https://irisbh.com.br/punicao-de-crimes-ciberneticos-em-2021-efeitos-das-alteracoes-na-lei-carolina-dieckmann/. Acesso em: 16 nov. 2024.

JESUS, D.; MILAGRE, J. A. **Manual de Crimes Informáticos**. 1ª ed. São Paulo: Saraiva, 2016.

MIGALHAS. **Sancionadas leis que tratam de crimes cibernéticos**. 2012. Disponível em: https://www.migalhas.com.br/quentes/168701/sancionadas-leis-que-tratam-de-crimes-ciberneticos. Acesso em: 17 out. 2024.

POLÍCIA CIVIL DO ESTADO DE GOIÁS. Policiais civis se capacitam no combate à exploração sexual. **ESCOLA SUPERIOR DA POLÍCIA CIVIL – ESPC A CASA DO POLICIAL CIVIL**. Disponível em: https://espc.policiacivil.go.gov.br/noticias/policiais-civis-se-capacitam-no-combate-a-exploracao-sexual. Acesso em: 18 out. 2024.

PRODANOV, C. C.; FREITAS, E. C. **Metodologia do Trabalho Científico:** Métodos e Técnicas da Pesquisa e do Trabalho Acadêmico. 2ª ed. Novo Hamburgo: Feevale, 2013.

SAFERNET BRASIL**. Indicadores da SaferNet**. Disponível em: https://indicadores.safernet.org.br/. Acesso em: 1 abr. 2025.

SILVA, C. B.; OLIVEIRA, L. L. **A responsabilidade civil na internet à luz do Marco Civil da Internet e julgados do Superior Tribunal de Justiça**. São Luís: Instituto de Ensino Superior do Sul do Maranhão – IESMA/Unisulma, 2023.

WENDT, E.; JORGE, H. V. N. **Crimes Cibernéticos:** Ameaças e procedimentos de investigação. 3ª ed. Rio de Janeiro: Brasport, 2021.