DESAFIOS PARA O DIREITO PENAL NA ERA DIGITAL: INVESTIGAÇÃO DAS DIFICULDADES ENFRENTADAS PELA LEGISLAÇÃO PENAL AO LIDAR COM CRIMES COMO FRAUDES ONLINE, HACKING E INVASÃO DE PRIVACIDADE

CHALLENGES FOR CRIMINAL LAW IN THE DIGITAL AGE: INVESTIGATION OF THE DIFFICULTIES FACED BY CRIMINAL LAW IN DEALING WITH CRIMES SUCH AS ONLINE FRAUD, HACKING AND INVASION OF PRIVACY

Bruno Gomes leal de Sá, Vinicius Sousa Trindade da Costa, Fabricio Sumar Ramos
Graduando do Curso de Direito do Centro Universitário São Jose. Email: Brunoleal536@gmail.com
Bianca Freire.
Entusiasta do Direito e educadora. Especializada em Penal, Processo Penal e Militar, também atuando como advogada da @lihduerj. Doutora em Direito pela UERJ e membro ativa da @comissaodedireitomilitar da OAB.

RESUMO

O objetivo deste estudo é investigar os desafios enfrentados pelo Direito Penal na era digital, especificamente no que se refere à legislação penal aplicada a crimes cibernéticos como fraudes online, hacking e invasão de privacidade. O estudo visa analisar as limitações das normas penais atuais, a eficácia das medidas jurídicas adotadas e as possíveis necessidades de reformas legislativas para enfrentar de forma mais eficaz essas novas modalidades de crime. A pesquisa será conduzida por meio de uma revisão bibliográfica, focando em literatura acadêmica, artigos jurídicos e estudos de caso relacionados à legislação penal e crimes cibernéticos. A revisão será realizada utilizando-se bases de dados especializadas em Direito, com a análise crítica de fontes primárias e secundárias para compreender as abordagens teóricas e práticas sobre o tema. Serão também exploradas as divergências na aplicação da lei em diferentes jurisdições, bem como as lacunas na legislação atual. Os desafios enfrentados pelo Direito Penal na era digital revelam a necessidade urgente de adaptação das normas jurídicas tradicionais para lidar com crimes cibernéticos complexos e em constante evolução. A revisão bibliográfica demonstra que, apesar dos avanços tecnológicos, a legislação penal ainda carece de mecanismos eficazes para combater de maneira eficiente crimes como fraudes online, hacking e invasão de privacidade. A modernização das leis e a capacitação das autoridades são essenciais para proteger os direitos dos indivíduos e garantir a segurança no ambiente digital.

Palavras-chave: Direito Penal Digital; Crimes Cibernéticos; Fraudes Online.

ABSTRACT

The aim of this study is to investigate the challenges faced by criminal law in the digital age, specifically with regard to criminal legislation applied to cybercrimes such as online fraud, hacking and invasion of privacy. The study aims to analyze the limitations of current criminal laws, the effectiveness of legal measures adopted and the possible need for legislative reforms to more effectively address these new types of crime. The research will be conducted through a literature review, focusing on academic literature, legal articles and case studies related to criminal law and cybercrimes. The review will be carried out using specialized legal databases, with a critical analysis of primary and secondary sources to understand theoretical and practical approaches to the subject. It will also explore the divergences in the application of the law in different jurisdictions, as well as the gaps in current legislation. The challenges faced by criminal law in the digital age reveal the urgent need to adapt traditional legal norms to deal with complex and constantly evolving cybercrimes. The literature review shows that, despite technological advances, criminal legislation still lacks effective mechanisms to efficiently combat crimes such as online fraud, hacking and invasion of privacy. Modernizing laws and training authorities are essential to protect the rights of individuals and ensuring security in the digital environment.

Keywords: Digital Criminal Law; Cybercrimes; Online Fraud.

INTRODUÇÃO:

Com o crescimento exponencial das tecnologias digitais, os crimes cibernéticos têm se tornado cada vez mais frequentes e sofisticados, desafiando a capacidade do Direito Penal de proporcionar uma resposta eficaz. A legislação tradicional, muitas vezes, não consegue acompanhar a velocidade das inovações tecnológicas, deixando lacunas na proteção dos direitos fundamentais. Embora a Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, tenha sido um avanço ao tipificar crimes cibernéticos no Brasil, ela ainda é insuficiente para cobrir a amplitude e a complexidade das infrações digitais. Diante disso, este estudo é justificado pela necessidade urgente de adaptação do sistema jurídico para enfrentar essas novas modalidades de crime, garantindo segurança e justiça no ambiente digital.

Um crime tradicional se refere a um ato que viola uma lei que o proíbe ou o obriga, resultando em penalidades após a condenação. Em termos mais simples, pode-se dizer que "crime é algo que é contra a lei". Como fenômeno social e econômico, o crime existe ao lado da sociedade humana. É um conceito legal que é sustentado por lei. Uma infração ou crime representa um dano legal que pode desencadear um processo criminal, potencialmente levando à punição (Damásio; Milagre, 2016).

Por outro lado, o crime cibernético, conforme definido por Nucci (2017), envolve ações em que o infrator se envolve em atividades ilegais com intenção negligente ou comete crimes em um contexto virtual. Os criminosos cibernéticos podem incluir infratores motivados, hackers organizados, funcionários descontentes e terroristas cibernéticos.

O problema central a ser abordado é a inadequação da legislação penal atual para lidar com crimes cibernéticos complexos, o que compromete a eficácia do sistema jurídico na era digital. Embora o Marco Civil da Internet (Lei nº 12.965/2014) estabeleça diretrizes importantes para o uso da internet no Brasil, ele não aborda suficientemente as questões criminais relacionadas à cibersegurança. A pergunta norteadora que guia esta pesquisa é: Como o Direito Penal pode ser aprimorado para enfrentar de forma mais eficaz os desafios impostos pelos crimes cibernéticos? Este questionamento direciona a investigação e orienta a análise das dificuldades enfrentadas pelo sistema jurídico.

Para alcançar uma resposta, este estudo tem como objetivo geral investigar os desafios enfrentados pelo Direito Penal na era digital, com foco em crimes cibernéticos como fraudes online, hacking e invasão de privacidade. Os objetivos específicos incluem analisar a eficácia da legislação penal atual, identificar as principais dificuldades na aplicação das normas jurídicas a crimes cibernéticos e propor possíveis reformas legislativas para aprimorar a proteção jurídica no ambiente digital. A análise considerará, entre outras, as limitações da Lei nº 12.737/2012 e as lacunas no Marco Civil da Internet, bem como a necessidade de incorporar novos instrumentos legais para tratar de crimes como hacking e invasão de privacidade.

A metodologia adotada consiste em uma revisão bibliográfica, onde serão analisadas fontes primárias e secundárias para examinar a literatura existente sobre legislação penal e crimes cibernéticos. A pesquisa revisará artigos acadêmicos, livros, jurisprudências e estudos de caso que abordem os desafios do Direito Penal na era digital, além de explorar propostas de reforma legislativa que possam contribuir para uma melhor resposta jurídica a esses crimes. Serão considerados textos como a Lei nº 12.737/2012 e o Marco Civil da Internet, além de análises comparativas com legislações estrangeiras que oferecem perspectivas sobre como o Brasil pode avançar na proteção contra crimes cibernéticos.

O estudo será organizado em torno de quatro tópicos principais, que se interligam para fornecer uma compreensão abrangente do problema. Primeiro, será analisada a Crimes Cibernéticos, discutindo o histórico e desenvolvimento desses crimes e como a tecnologia tem influenciado sua natureza. A relevância de normas como o Decreto-Lei nº 2.848/1940 (Código Penal) será considerada, particularmente no que diz respeito às adaptações necessárias para os tempos digitais. Em seguida, a seção sobre Legislação Penal e Crimes Cibernéticos realizará uma análise crítica da legislação penal atual, destacando suas limitações e lacunas na resposta a crimes cibernéticos, com foco em leis como a Lei nº 12.737/2012 e o Marco Civil da Internet. A terceira parte abordará os Desafios Específicos do Direito Penal na Era Digital, tratando das dificuldades enfrentadas na aplicação das leis tradicionais a crimes digitais, como questões de jurisdição, coleta de provas e identificação de criminosos. Por fim, será examinado o Impacto Social dos Crimes Cibernéticos, explorando as consequências sociais e econômicas desses crimes e a percepção pública sobre a segurança digital e a confiança nas instituições jurídicas. Essas análises são essenciais para compreender como o Direito Penal precisa evoluir para enfrentar os desafios impostos pelo avanço tecnológico e garantir a proteção dos direitos fundamentais no ambiente digital, oferecendo assim uma resposta mais eficaz aos crimes cibernéticos.

FUNDAMENTAÇÃO TEÓRICA

Crimes Cibernéticos

O crime cibernético surgiu pela primeira vez em meados da década de 1960, caracterizado por atos de manipulação, sabotagem, espionagem ou abuso de computador. Em meados da década de 1980, conforme as mudanças sociais e econômicas se desenrolavam, houve um aumento notável nas atividades criminosas online. Esse aumento foi evidente em áreas como manipulação de contas bancárias,

pirataria de software, pornografia infantil e abuso de telecomunicações, que começaram a levantar preocupações entre os cidadãos naquela época (Oliveira Júnior, 2013).

O termo “crime cibernético” ganhou amplo reconhecimento apenas no final da década de 1990, durante uma reunião do G-8 focada em abordar atividades ilegais online, incluindo discussões sobre potenciais estratégias de prevenção e penalidades. Após essa reunião, o termo começou a se referir especificamente a atos criminosos realizados no reino digital. A progressão dessas infrações se alinha com o avanço contínuo da tecnologia, complicando os esforços para combatê-las (Pinheiro, 2000).

Em muitos casos, o objetivo desses criminosos são informações digitais, que eles obtêm por meio de diferentes formas de malware, incluindo spyware e um tipo específico conhecido como keyloggers. Conforme observado por Jesus e Milagre (2016), os keyloggers desempenham um papel crucial na captura de dados que os usuários inserem ao visitar sites como internet banking ou plataformas de e-commerce.

Conforme declarado pelo CERT.BR (2012), o ransomware é uma forma de malware que torna os dados em um dispositivo inacessíveis ao empregar criptografia e exigir pagamento para recuperar o acesso. Além de afetar o dispositivo inicial, o ransomware também verifica se há dispositivos adicionais vinculados à rede e os criptografa também. O pagamento do resgate é normalmente solicitado em bitcoins, que são difíceis de rastrear. O ransomware pode ser categorizado em dois tipos: Locker, que bloqueia o acesso ao próprio dispositivo infectado, e Crypto, que restringe o acesso aos dados armazenados no dispositivo infectado, principalmente por meio de criptografia.

Juntamente com os traços associados a crimes "reais", os crimes no reino virtual são reconhecidos como aqueles perpetrados por meio de dispositivos tecnológicos. A Organização para Cooperação e Desenvolvimento Econômico (OCDE) das Nações Unidas forneceu uma definição de crime cibernético em 1983, descrevendo-o como "qualquer conduta ilegal, antiética ou não autorizada envolvendo processamento automático de dados e/ou transmissão de dados" (Palazzi, 2000).

Os crimes cibernéticos são categorizados em dois tipos: apropriados e impróprios. O primeiro se refere a ações ilegais e culpáveis que buscam especificamente comprometer um sistema de computador ou seus dados, prejudicando sua confiabilidade, integridade ou disponibilidade; os hackers servem como um exemplo prevalente disso.

Em contraste, os crimes cibernéticos impróprios envolvem comportamentos típicos, ilegais e culpáveis que utilizam mecanismos de computador como instrumentos, mas poderiam ter sido executados por métodos alternativos, como no caso do "Discurso de Ódio" (Palazzi, 2000).

Semelhante à forma como as atividades criminosas tradicionais evoluem ao longo do tempo, os crimes cibernéticos também estão adotando novas formas devido aos avanços tecnológicos que apoiam e aprimoram sua execução. À medida que o número de usuários da Internet ultrapassa 4,66 bilhões, identificar os indivíduos responsáveis por crimes online está se tornando cada vez mais desafiador (Palazzi, 2000).

O conceito de crimes cibernéticos é relativamente novo quando comparado aos crimes tradicionais, que vêm sendo examinados há um período considerável. Uma definição bem conhecida é fornecida por Krone (2005), que descreve os crimes cibernéticos como abrangendo uma gama de atividades criminosas que têm como alvo dados, bem como violações relacionadas a conteúdo e direitos autorais. No entanto, essa definição é mais ampla e abrange delitos como fraude, acesso não autorizado, pornografia infantil e assédio online. Os crimes cibernéticos são caracterizados como crimes de meio, utilizando o ambiente virtual para sua execução. Em sua obra “Crimes virtuales, vviagens” (Crimes virtuais, vítimas reais), Moisés Cassanti define crimes cibernéticos como "qualquer atividade em que um computador ou uma rede de computadores é usada como ferramenta, base para ataque ou como meio de crime" (Oliveira Júnior, 2013).

Assim, pode-se afirmar que os crimes cibernéticos abrangem todas as atividades que ocorrem por meios virtuais, utilizadas para perpetrar atos ilícitos, seja reformulando a execução de crimes tradicionais ou dando origem a novos delitos. Vários métodos são empregados pelos criminosos cibernéticos para realizar suas atividades ilícitas (Pinheiro, 2000).

Legislação Penal e Crimes Cibernéticos

A Lei 12.737/2012 introduziu um avanço legislativo que incorporou o crime conhecido como “Invasão de dispositivo de computador” ao Código Penal Brasileiro, adicionando os artigos 154-A e 154-B. Além disso, revisou os artigos 266 e 298 para abranger crimes cometidos por meios de computador dentro do arcabouço do direito penal. Consequentemente, o texto legal é articulado da seguinte forma.

Como resultado, o sistema legal brasileiro incluiu uma disposição para o crime de acesso ilícito ao dispositivo de outra pessoa sem justificativa ou permissão do proprietário, com pena de três meses a um ano. Esta pena pode ser aumentada se a invasão resultou em dano econômico à vítima ou envolveu a administração pública como parte afetada.

O bem legal que é salvaguardado diz respeito à violação da liberdade de um usuário de dispositivo de computador, executada por meio de outro dispositivo de computador (Nucci, 2014). Este crime é prevalente e pode ser perpetrado por qualquer pessoa, pois não necessita de nenhuma habilidade ou status específico do infrator; ou seja, o autor não precisa ser um especialista, comumente chamado de hacker (Junior, 2013; Nucci, 2014).

Além disso, o sujeito passivo pode incluir qualquer pessoa responsável pelo bem jurídico violado, independentemente de ser o proprietário ou detentor do bem, como em situações em que empresas fornecem equipamentos a seus funcionários (Reis, 2014).

Para defini-lo, a intenção é crucial (portanto, a forma negligente não é relevante), juntamente com o objetivo específico da ação, que inclui "a aquisição, manipulação ou destruição de dados ou informações, bem como a obtenção de vantagem ilícita" (Reis, 2014).

Em 2021, a legislação brasileira foi revisada, em especial com a promulgação da Lei 14.555/2021. A Lei Geral de Proteção de Dados, promulgada em 2018, entrou em vigor apenas em 2020. Inspirada no Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, essa lei tem como objetivo proteger os direitos fundamentais de liberdade e privacidade, bem como o desenvolvimento da pessoa natural (Brasil, 2020).

O objetivo desta lei é criar clareza jurídica por meio da implementação de regulamentações e práticas que protejam os dados pessoais de todos dentro do território brasileiro, de acordo com os padrões internacionais estabelecidos.

A LGPD estabelece regras sobre o uso, proteção e transferência de dados pessoais no Brasil nos setores público e privado. Ela define explicitamente as partes envolvidas, delineando suas funções, responsabilidades e potenciais penalidades no domínio civil, que podem chegar a multas de até 50 milhões de reais para cada incidente. (Somadossi; Henrique, 2018).

A legislação brasileira estabelece diretrizes claras para a proteção de dados, especificando o que é considerado dado pessoal e identificando informações sensíveis que requerem maior proteção, como os dados de crianças e adolescentes. Observa-se que os crimes cibernéticos têm aumentado significativamente, com o surgimento de métodos inovadores, especialmente durante a pandemia de COVID-19, que afetou drasticamente o mundo, modificando as rotinas e a maneira como diversas atividades são realizadas. Em 31 de março de 2021, a Lei 14.132/21 foi promulgada, introduzindo uma mudança legislativa importante ao adicionar o artigo 147-A ao Código Penal, tornando o stalking uma infração criminal.

Conforme articulado por Castro e Sydrow (2017), stalking se refere ao termo inglês usado para alguém que persistente e obsessivamente assedia outro indivíduo; ele incorpora o comportamento de espionar e perseguir alguém continuamente. Os autores elaboram ainda que esse comportamento constitui uma forma de assédio marcada pela insistência, impertinência e engajamento habitual por meio de qualquer meio de contato, vigilância, perseguição ou assédio. Em novembro de 2019, a senadora Leila Barros apresentou um projeto de lei que visa criminalizar tais ações. Com o surgimento da tecnologia e o uso generalizado das mídias sociais, novos tipos de crimes surgiram, necessitando de melhorias no Código Penal para oferecer maior proteção às vítimas de comportamento que muitas vezes transita do assédio online para o stalking físico (Brasil, 2021). Posteriormente, o presidente Jair Bolsonaro sancionou o projeto de lei em março de 2021, que entrou em vigor em 1º de abril do mesmo ano. Antes dessa legislação, tal conduta era meramente categorizada como infração penal pelo Artigo 65 da Lei de Contravenções Penais - Decreto-Lei 3.688, promulgado em 1941. Essa classificação foi revogada e definida como perturbação da paz alheia, com penas que variam de 15 dias a 2 meses de prisão e multa.

É crucial entender que para que o stalking seja considerado um ato criminoso, ele deve envolver comportamento repetido que leve a infrações adicionais, como intimidação ou ameaças ilegais, que podem prejudicar o bem-estar físico ou mental da vítima, perturbar seu estado emocional e incutir medo ou ansiedade (Barretos, 2021).

Conforme observado anteriormente, a Lei 14.155/2021 foi promulgada pelo governo federal no final de maio de 2021, resultando em alterações em certas disposições do Código Penal. Esta legislação introduz penalidades mais severas para crimes cibernéticos, incluindo invasão de dispositivos, fraude e roubo, particularmente aqueles perpetrados por meio de dispositivos eletrônicos como celulares, computadores e tablets, independentemente de sua conectividade com a internet. Consequentemente, esta lei oferece, ainda que marginalmente, proteção aprimorada para usuários no reino digital.

De acordo com a legislação vigente, o roubo qualificado cometido por meios eletrônicos, independentemente de envolver a violação de um mecanismo de segurança, o uso de software malicioso ou outros métodos fraudulentos, é punido com uma pena que varia de quatro a oito anos de prisão, além de multa. A lei também estabelece que, se o crime for direcionado a um idoso ou vulnerável, a punição pode ser aumentada de um terço até o dobro. Ademais, se o crime envolver o uso de um servidor de computador localizado fora do país, a pena pode ser elevada de um terço a dois terços. Além disso, a pena para fraude foi ampliada para um período de quatro a oito anos de prisão, juntamente com multa, especialmente quando a vítima é enganada e compartilha informações por meio de redes sociais. Essa pena pode ser agravada se o crime envolver um servidor fora do país ou for cometido contra um idoso ou vulnerável (Brasil, 2021).

Desafios Específicos do Direito Penal na Era Digital

Para salvaguardar efetivamente os direitos legais dos cidadãos, a lei deve se adaptar às mudanças de costumes, hábitos e modos de interação dentro da sociedade.

Nos dias de hoje, indivíduos que inicialmente não mostram sinais de envolvimento em comportamento criminoso exploram o anonimato percebido da World Wide Web para obter benefícios ilícitos de vários tipos ou para expressar frustrações e ódio pessoais (Lei nº 12.965/2014).

Assim, a própria Internet que significa avanços na comunicação, informação, ciência e comércio simultaneamente propaga uma falsa sensação de impunidade. Isso ocorre devido a fatores como anonimato, desafios na identificação de infratores e as complexidades envolvidas na aplicação das leis existentes. É importante destacar que várias ferramentas tecnológicas já estão disponíveis para salvaguardar os interesses legais na World Wide Web. Entre elas estão: controle de acesso dividido em autenticação e autorização; mecanismos de defesa compostos por sistemas que reforçam a adesão às políticas de controle de acesso; "Redes Privadas Virtuais", que facilitam a troca segura de informações em redes públicas; monitoramento de arquivos de log produzidos por serviços de rede; sistemas que integram hardware e software projetados para captura de informações; bem como criptografia e assinaturas digitais (Domingues; Finkeltein, 2003).

Os desafios que devem ser enfrentados para que a Internet sirva genuinamente como uma rede de avanço para benefício da comunidade incluem a ausência de incentivos efetivos para a criação de programas mais avançados e a subvalorização de profissionais de tecnologia. Além disso, é evidente que as leis tradicionais não evoluíram junto com as novas tecnologias, destacando a necessidade de melhorias na legislação que rege todos os processos criminais relacionados a crimes cibernéticos. Sem essas melhorias, o processo corre o risco de falhar devido a questões como evidências insuficientes sobre materialidade ou autoria, ou complicações decorrentes do estatuto de limitações, conforme observado na Lei nº 12.965/2014.

Em última análise, um primeiro passo essencial na prevenção e gerenciamento de atividades criminosas no âmbito online é promover a conscientização entre o público sobre o uso responsável e moderado da Internet, aderindo aos limites constitucionais e respeitando os direitos de si mesmo e dos outros (Lei nº 12.965/2014).

Considerando os pontos acima mencionados, pode-se identificar que a convulsão social e tecnológica instigada pela Internet tem imposto desafios ao Direito. Isso se deve ao surgimento de novas situações e comportamentos que impactam os bens jurídicos,

necessitando de uma rápida adaptação da legislação. No entanto, o Brasil está significativamente atrasado no âmbito da legislação sobre crimes relacionados à informática (Jesus; Milagres, 2016, p. 70). As regulamentações são fragmentadas em disposições legais gerais e específicas, dificultando o acesso às regras aplicáveis.

Consequentemente, a doutrina enfatiza a necessidade de estabelecer uma legislação específica que consolide em um código distinto a maioria dos artigos relacionados aos crimes cibernéticos, o que aumentaria sua acessibilidade e aplicabilidade para profissionais do direito, autoridades competentes e a sociedade em geral. No entanto, alguns especialistas argumentam que essa nova legislação seria desnecessária, uma vez que acreditam que o Código Penal Brasileiro já abrange a maioria dos crimes cibernéticos. Essa perspectiva é compartilhada por Alexandre Jean Daoun, que critica a compulsividade de legislar e criar leis penais, ressaltando que o Direito Penal é uma ferramenta extremamente severa, devendo ser aplicada de maneira mínima. Ele observa que, no ambiente digital, 95% das relações já são regidas por estatutos penais, o que reduz a necessidade de criar uma legislação penal específica para esses crimes (Jesus; Milagres, 2016).

Nesse contexto, o legislador criminal brasileiro parece estar mudando para implementar modificações direcionadas no Código Penal e no Código de Processo Penal, como evidenciado pela promulgação da Lei nº 12.737 em 30 de novembro de 2012, Lei nº 13.964 em 24 de dezembro de 2019, Lei nº 13.968 em 26 de dezembro de 2019, Lei nº 14.132 em 2021 (Lei do Stalking) e Lei nº 14.155 em 27 de maio de 2021, em vez de focar no estabelecimento de uma lei dedicada à regulamentação de crimes cibernéticos.

Independentemente disso, embora o desenvolvimento da previsão de crimes ocorridos em espaços virtuais seja reconhecido, é essencial avaliar sua eficácia, que Afonso da Silva (2007, p. 66) define como:

A eficácia se refere à capacidade de atingir metas que foram estabelecidas como objetivos. Quando se trata de normas jurídicas, a eficácia envolve a capacidade de cumprir os objetivos expressos nelas, o que, em última análise, envolve a implementação dos requisitos legais estabelecidos pelo legislador. Uma norma pode ter eficácia jurídica, mas não ter eficácia social; em outras palavras, pode produzir consequências jurídicas, como a anulação de normas anteriores, sem ser respeitada em nível social.

Independentemente disso, embora o desenvolvimento da previsão de crimes ocorridos em espaços virtuais seja reconhecido, é essencial avaliar sua eficácia, que, segundo Afonso da Silva, refere-se à capacidade de uma norma atingir as metas estabelecidas como objetivos. No contexto das normas jurídicas, a eficácia está relacionada à habilidade de cumprir os objetivos expressos na legislação, que em última análise, envolve a implementação dos requisitos legais determinados pelo legislador. Afonso da Silva destaca que uma norma pode ter eficácia jurídica, gerando efeitos legais como a revogação de normas anteriores, mas não necessariamente ser eficaz em termos sociais, ou seja, pode não ser cumprida ou respeitada na prática social (Silva, 2007).

Nesse contexto, o repositório do Centro Nacional de Denúncias de Crimes Cibernéticos, que resulta de uma colaboração entre o Ministério Público Federal (MPF), o Senado Federal, a Polícia Federal e a Organização Não Governamental Safernet Brasil, é apresentado como fonte de informação. A análise dos dados e a interpretação dos gráficos revelam que o Brasil ocupa o quinto lugar entre os países com maior número de endereços eletrônicos únicos reportados em 2021 (Datasafer, 2022).

Além disso, os relatos sobre pornografia infantil aumentaram notavelmente em 3,65% em comparação a 2020. Em 2021, houve 14.476 relatos anônimos relacionados ao neonazismo, refletindo um aumento significativo de 60,7% em relação ao ano anterior. Consequentemente, os dados coletados por meio da parceria relevante forneceram justificativa para a Comissão de Direitos Humanos e Minorias da Câmara dos Deputados aprovar o Projeto de Lei nº 2.496/2019, que visa ampliar o escopo de crimes de ódio perpetrados ou pretendidos por meio de plataformas digitais, para os quais a Polícia Federal é encarregada de investigar.

No decorrer do exame das regulamentações legais brasileiras destacadas no estudo, tornou-se evidente que certas modificações foram instituídas para facilitar o ajuste de infrações penais existentes no que se refere à execução online (Lei nº 12.737/2012; Lei nº 14.155/2021). No entanto, há uma necessidade reconhecida de atualizações contínuas na legislação, garantindo que o sistema jurídico brasileiro possua as ferramentas essenciais para lidar efetivamente com esses crimes. Quando faltam disposições específicas, a abordagem comum é alinhar o caso específico com as regulamentações legais mais relevantes (Lei nº 13.964/2019).

Consequentemente, a ausência de diretrizes claras pode resultar em penalidades que não correspondem adequadamente às consequências dos delitos cometidos, levando a percepções de leniência ao fatorar o impacto das ferramentas digitais. Esta avaliação destaca o reconhecimento de um grau de inadequação na legislação existente, pois as evidências estatísticas ressaltam a necessidade de leis mais rigorosas destinadas a coibir crimes que ocorrem no domínio cibernético (Lei nº 14.132/2021).

Diante desses fatores, é importante destacar a necessidade de colaboração entre agências estatais e o público, com este último buscando obter conscientização sobre os riscos associados ao ambiente virtual para reduzir sua suscetibilidade. Enquanto isso, o Estado adotaria uma abordagem repressiva ao fornecer uma estrutura legal bem definida, que poderia envolver tanto o estabelecimento de novas leis quanto a modificação das atuais. Essa estrutura incluiria penalidades que correspondem a crimes cibernéticos e infrações penais específicas adaptadas a contextos digitais, garantindo a responsabilização por crimes e, por sua vez, promovendo maior segurança jurídica (Lei nº 13.709/2018).

Impacto Social dos Crimes Cibernéticos

As repercussões sociais e psicológicas de crimes cometidos na Internet podem ser devastadoras, muitas vezes sujeitando as vítimas ao julgamento social e ao ridículo. Dado que as atividades criminosas nas redes sociais envolvem vários indivíduos interagindo globalmente, as consequências de tais crimes são vastas. Particularmente quando essas ofensas infringem o direito à liberdade, mesmo nos casos mais específicos e brandos, atos como fraude, estelionato e pedofilia têm como alvo indivíduos ou grupos específicos sem causar perturbação generalizada no reino virtual. É importante destacar que essas ofensas ocorrem silenciosamente, sem soar nenhum alarme (Castells, 2013).

No alvorecer do século XXI, houve um crescimento sem precedentes na tecnologia digital, particularmente nos reinos da informação, comunicação e compartilhamento de dados dentro do cenário virtual. Embora esse crescimento tenha introduzido inúmeros benefícios, também apresentou desafios que devem ser enfrentados à medida que a sociedade continua a evoluir (Schwab, 2019).

Conforme observado por Schwab (2019), estamos atualmente vivenciando a quarta revolução industrial, também conhecida como Indústria 4.0. Esta fase é caracterizada pelo avanço e aplicação de tecnologias projetadas para compartilhamento de informações, impulsionadas pelo surgimento de algoritmos matemáticos e suas aplicações inovadoras em automação robótica e inteligência artificial. Embora essa tendência esteja inegavelmente transformando interações sociais e empresariais, o autor sugere que ela permanece em sua infância, tornando difícil prever o resultado desse novo movimento, que está enraizado no reino virtual da internet.

De acordo com Castells (2013), o cenário de compartilhamento de dados online incorporou características da sociedade tradicional, coincidindo com o surgimento de conflitos e desafios do mundo físico para o espaço virtual, o que traz vantagens e problemas nas interações sociais.

Assim, o crime evoluiu dentro do cenário digital, fomentando fraudes econômicas, espionagem e roubo de segredos de empresas, indústrias e instituições para obter vantagens injustas nos reinos econômico e político-ideológico (Castells, 2013).

Perrin (2005) afirma que o cenário virtual facilitou o surgimento do crime cibernético, um termo que abrange as várias questões criminais que se desenvolveram e proliferaram no âmbito online, impactando significativamente as informações de indivíduos e organizações ao mesmo tempo em que se intrometem na vida das pessoas.

Da mesma forma, Simas (2014, p. 12) aponta que o crime cibernético surge como um “fenômeno do crime de computador [...], ações que infringem direitos básicos, seja empregando tecnologia da informação para realizar um crime ou como um componente de delitos legalmente definidos”, particularmente em um contexto virtual em vez do âmbito físico visto em modelos tradicionais.

De acordo com Castells (2013), o crime tradicional adaptou seu modelo operacional, mudando de um espaço físico claramente definido para explorar

vulnerabilidades no cenário digital da internet, em meio ao surgimento de tecnologias avançadas ou disruptivas relacionadas a negócios e atividades corporativas.

O objetivo de se envolver em atividades criminosas e obter benefícios injustos pela internet transformou o conceito de crime, tanto em termos de geografia quanto de métodos. Essa evolução ocorre por meio de ações solitárias ou de grupos sofisticados do crime organizado, ambos empregando táticas tecnológicas avançadas para atingir indivíduos, organizações e empresas no mundo digital (Castells, 2013).

Conforme observado por Moisés de Oliveira Cassanti (2014), os crimes cibernéticos abrangem um tipo específico de comportamento criminoso que inclui duas categorias principais de usuários on-line potencialmente criminosos: hackers e crackers. Embora "hacker" seja um termo frequentemente associado a crimes virtuais, Cassanti enfatiza que os verdadeiros infratores são, de fato, crackers. A diferença entre esses tipos de usuários está enraizada na aplicação de conhecimento tecnológico, ou "know-how", que consiste em conhecimento prático, incluindo fórmulas secretas, técnicas tecnológicas e procedimentos.

Hackers são programadores qualificados com ampla experiência em tecnologia e Internet; no entanto, eles normalmente não aplicam suas habilidades para atividades ilegais no início (Cassanti, 2014).

Crackers, um termo originário do verbo inglês "to crack", referindo-se ao ato de quebrar, se envolvem em atividades como violar sistemas de segurança, decifrar códigos de criptografia e quebrar senhas para acessar redes ilegalmente. Sua intenção é se infiltrar e interromper sistemas e dispositivos eletrônicos para ganho ilícito (Cassanti, 2014).

Conforme observado por Rossini (2004), a Conferência das Nações Unidas sobre Comércio e Desenvolvimento revela que o Brasil ocupa a quarta posição em número de usuários da Internet. Dada essa base substancial de usuários, não é surpreendente que haja uma prevalência significativa de crimes cibernéticos, com novos golpes sendo introduzidos continuamente e vários métodos de acesso a informações pessoais em constante evolução.

Este tópico visa explorar vários crimes que podem ser perpetrados pela Internet, redes de computadores e dispositivos móveis. O Código Penal, originário de 1940, foi

elaborado em um contexto diferente daquele em que vivemos atualmente. Como resultado, tornou-se essencial ao longo do tempo implementar modificações, ajustes e o estabelecimento de legislação específica para abordar os vazios deixados por certas leis existentes (Maues; Duarte; Cardoso, 2018).

Ao avaliar crimes cibernéticos, o Código Penal identifica tipos distintos que dependem da Internet para execução, visando principalmente infringir informações. Além disso, existem crimes cibernéticos impróprios que necessitam de tecnologia e software sofisticado para sua comissão (Maues; Duarte; Cardoso, 2018).

O artigo 138 do Código Penal (Brasil, 1940) trata da calúnia, tipificando como crime o ato de fazer falsas declarações sobre alguém atribuindo-lhe fato específico considerado criminoso. O artigo 139 do mesmo código trata da difamação, definindo como crime difamar alguém atribuindo-lhe fato que lhe lesa a reputação. Já o artigo 140 do Código Penal (Brasil, 1940) trata da injúria, definindo como crime ofender alguém, atentando contra sua dignidade ou decoro.

CONSIDERAÇÕES FINAIS

A necessidade de adaptar o arcabouço legal brasileiro para atender aos desafios contemporâneos apresentados pela era digital é evidente em todas as discussões e avaliações. Em um ambiente hiperconectado e globalizado, a disseminação de informações traz oportunidades e desafios consideráveis, principalmente no que diz respeito à proliferação de notícias falsas e à ocorrência de crimes cibernéticos. Os esforços do governo brasileiro para enfrentar essa realidade por meio de iniciativas legislativas como o Projeto de Lei das Notícias Falsas destacam a necessidade urgente de medidas de proteção eficazes contra atividades online prejudiciais.

As discussões sobre o Projeto de Lei 2630/2020 são profundamente influenciadas pela tensão entre proteger a sociedade das ameaças representadas pela desinformação e defender direitos essenciais como privacidade e liberdade de expressão. Essa

interação ressalta a complexidade envolvida na legislação em um reino tão fluido quanto o cenário digital. Cada sugestão delineada no projeto de lei exige exame completo e deliberação cuidadosa para garantir que os interesses da comunidade sejam abordados e, ao mesmo tempo, proteger os direitos individuais.

No âmbito dos crimes cibernéticos, é evidente que o arcabouço legal existente, apesar do progresso feito, continua a encontrar obstáculos devido ao ritmo rápido do avanço tecnológico e ao caráter global do ciberespaço. O sentimento de impunidade, frequentemente aumentado pelos desafios na identificação e no julgamento de infratores, ressalta a necessidade de métodos investigativos aprimorados e maior colaboração internacional para abordar essas questões de forma eficaz.

Consequentemente, a importância das evidências em crimes cibernéticos foi identificada como um aspecto vital. Questões em torno da preservação de evidências digitais e sua aceitação em processos judiciais exigem consideração cuidadosa e modificações dentro do arcabouço legal para garantir a justiça e a eficácia das condenações. As características únicas do reino digital exigem uma estratégia legal personalizada que leve em consideração tanto as nuances tecnológicas quanto as proteções processuais estabelecidas.

O âmbito dos crimes cibernéticos e da desinformação no Brasil está em constante evolução e exige atenção cuidadosa do sistema legal. Uma relação harmoniosa entre tecnologia, sociedade e legislação é necessária para garantir uma internet segura, equitativa e irrestrita para todos os usuários. A busca por esse equilíbrio, como demonstrado, representa uma jornada crucial e contínua no cenário atual.

O avanço da tecnologia, a interconexão econômica, o uso generalizado de computadores na sociedade e a ampla influência da Ciência da Computação obrigaram a Ciência Criminal contemporânea a analisar as atividades criminosas interligadas à computação.

Os crimes cibernéticos constituem atividades ilegais que ocorrem on-line, infringindo os direitos de propriedade intelectual de indivíduos, organizações e do Estado como um todo. O aumento de tais delitos é evidente diariamente, muitas vezes decorrente da negligência dos usuários em relação à proteção de dados. Consequentemente, os criminosos cibernéticos aproveitam as oportunidades para obter

informações que colocam em risco a integridade e a estabilidade das organizações que possuem esses dados.

Houve um aumento constante dessas atividades em todos os níveis do ciberespaço. Aqueles que se envolvem nessa forma de crime desenvolvem e implementam várias técnicas que os permitem realizar delitos como roubo, fraude e chantagem, ao mesmo tempo em que comprometem a privacidade e a identidade de indivíduos, organizações e até mesmo governos. Consequentemente, a importância de criar um sistema de segurança para proteger informações confidenciais está se tornando cada vez mais crucial, principalmente quando os dados envolvidos estão sob jurisdição privilegiada.

O Brasil, assim como outras nações, enfrenta o desafio de lidar com o crime cibernético e, ao mesmo tempo, garantir a segurança de seus cidadãos e organizações. Esse tipo de crime pode ocorrer sem levar em conta fronteiras geográficas e acontece em um reino virtual, complicando o processo de infratores. Portanto, uma abordagem global unificada é essencial para lidar com a questão do crime cibernético em escala internacional. O progresso legislativo foi feito por meio de várias leis, incluindo a Lei 12.735/2012, Lei n.º 12.737/2012, Lei 12.965, Lei 13.260/2016, Lei n.º 13.709/2018 e Lei n.º 14.155/2021, todas voltadas para a proteção de vítimas de crimes cibernéticos, sejam pessoas físicas ou jurídicas. Isso reflete uma preocupação genuína entre os legisladores em defender e defender os direitos dos cidadãos; no entanto, a eficácia dessas medidas fica aquém das expectativas, pois o crime cibernético é inerentemente transnacional, conforme discutido ao longo deste estudo, cruzando várias fronteiras.

Considerando a efetividade da norma, surge um desafio que reflete a incapacidade das instituições nacionais de proporcionar aos cidadãos proteção judicial adequada aos seus direitos nesse contexto.

REFERÊNCIAS

BARRETOS, A. Crimes Cibernéticos e a Legislação Brasileira: Um Estudo Sobre o Stalking. São Paulo: Saraiva, 2021.

BRASIL. Constituição da República Federativa do Brasil. Brasília: Senado, 1988. Disponível em: https://www2.senado.leg.br/bdsf/bitstream/handle/id/518231/CF88_Livro_EC91_2016.pdf. Acesso em: 29 ago. 2024.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. Diário Oficial da União: seção 1, Rio de Janeiro, p. 1, 31 dez. 1940. Disponível em: https://www2.camara.leg.br/legin/fed/declei/1940-1949/decreto-lei-2848-7-dezembro-1940-412868-norma-pe.html. Acesso em: 29 ago. 2024.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências. Diário Oficial da União: seção 1, Brasília, DF, p. 1, 03 dez. 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 29 ago. 2024.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil – Marco Civil da Internet. Diário Oficial da União: seção 1, Brasília, DF, p. 1, 24 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 29 ago. 2024.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 29 ago. 2024.

BRASIL. Lei nº 13.964, de 24 de dezembro de 2019. Aperfeiçoa a legislação penal e processual penal. Diário Oficial da União, Brasília, DF, 24 dez. 2019. Disponível em:

http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13964.htm. Acesso em: 29 ago. 2024.

BRASIL. Lei nº 14.132, de 31 de março de 2021. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, para dispor sobre o crime de perseguição. Diário Oficial da União, Brasília, DF, 31 mar. 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14132.htm. Acesso em: 29 ago. 2024.

BRASIL. Lei nº 14.155, de 27 de maio de 2021. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, para agravar a punição do crime de fraude eletrônica e dispor sobre o crime de invasão de dispositivo informático. Diário Oficial da União, Brasília, DF, 27 maio 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm. Acesso em: 29 ago. 2024.

CASSANTI, Moisés de Oliveira. Crimes virtuais, vítimas reais. 1. ed. Rio de Janeiro: Brasport, 2014.

CASTELLS, Manuel. A sociedade em rede. In: A era da informação: economia, sociedade e cultura – volume I. 6ª ed. São Paulo: Paz e Terra, 2013.

CERT.BR. Cartilha de segurança para internet. Disponível em: https://cartilha.cert.br/ransomware/. Acesso em: 29 ago. 2024.

DAMÁSIO, José Antonio. Manual de Crimes Informáticos. São Paulo: Saraiva, 2016.

DATASAFER. Indicadores da Central Nacional de Denúncias de Crimes Cibernéticos. Disponível em: https://indicadores.safernet.org.br/. Acesso em: 29 ago. 2024.

DOMINGUES, Alessandra de Azevedo e FINKELTEIN, Maria Eugênia (Organização). DIREITO & INTERNET - Aspectos jurídicos relevantes. São Paulo, 2003: Quarter Latin, pgs. 378/379.

JESUS, Damásio de; MILAGRE, José Antônio. Manual de crimes informáticos. São Paulo: Saraiva, 2016.

JUNIOR, M. de S. Invasão de Dispositivos Informáticos: Aspectos Jurídicos e Práticos. São Paulo: Revista dos Tribunais, 2013.

KRONE, T. High tech crime brief: Cybercrime and digital evidence. Australian Institute of Criminology, 2005. Disponível em: https://aic.gov.au/publications/tandi/tandi290. Acesso em: 29 ago. 2024.

MAUES, Sidnei; DUARTE, Paulo; CARDOSO, Juliana. Direito digital: fundamentos, práticas e reflexões. Rio de Janeiro: Forense, 2018.

NUCCI, Guilherme de Souza. Código Penal comentado, 17° Edição. Rio de Janeiro: Forense, 2017.

OLIVEIRA JÚNIOR, M. Crimes cibernéticos: aspectos gerais e jurídicos. 2. ed. São Paulo: Saraiva, 2013.

PALAZZI, E. Cybercrime: uma visão panorâmica. São Paulo: Atlas, 2000.

PERRIN, Stephanie. O cibercrime. In: AMBROSI, Alain; PEUGEOT, Valérie; PIMIENTA, Daniel. Desafios de Palavras: enfoques multiculturais sobre as sociedades da informação. C&F Éditions, 2005.

PINHEIRO, J. Direito penal e novas tecnologias. 2. ed. Rio de Janeiro: Forense, 2000.

REIS, L. Crimes Informáticos: Teoria e Prática. 2. ed. Curitiba: Juruá, 2014.

ROSSINI, Fabio. Informática, telemática e direito penal. São Paulo: Memória Jurídica, 2004.

SCHWAB, Klaus. A quarta revolução industrial. Edipro, 2019.

SILVA, José Afonso. Aplicabilidade das Normas Constitucionais. 8. ed. São Paulo: Malheiros, 2012.

SIMAS, Diana Viveiros de. O cibercrime. 2014. Dissertação (Mestrado em Ciências Jurídico Forenses) - Universidade Lusófona de Humanidades e Tecnologias, Lisboa, 2014.

SOMADOSSI, H. Lei Geral de Proteção de Dados: Comentários e Aplicações. Brasília: Editora do Brasil, 2018. Disponível em: https://www.lgpdonline.com.br. Acesso em: 29 ago. 2024.