

ANÁLISE EVOLUTIVA DOS CRIMES CIBERNÉTICOS E A LEGISLAÇÃO PENAL BRASILEIRA

Vilma Maria Marcelli

Professora; bacharel em Direito do Centro Universitário de Paulínia

Roberto José Daher

Coordenador e Professor do Curso de Direito do Centro Universitário de Paulínia; Advogado, Delegado de Polícia aposentado. Bacharel em Ciências Jurídicas e Sociais pela PUC de Campinas, Especialista em Polícia Judiciária e Sistema de Justiça Criminal pela Academia de Polícia, Mestre em Direito Constitucional pela UNIP – Campinas (roberto.daher@facp.com.br)

RESUMO

O presente estudo realiza uma investigação sobre o surgimento dos crimes cibernéticos e os conceitos atuais dessa nova forma de criminalidade, que surge em decorrência das inovações tecnológicas, da globalização e da ampla disseminação de novos conteúdos tecnológicos. O objetivo é analisar a evolução do Direito brasileiro no tratamento das condutas delitivas frente aos crimes cibernéticos e o tratamento que o Judiciário realiza nesse contexto. No contexto do ciberespaço, serão discutidas as fraudes virtuais, crime instituto que figura entre os mais impactantes no ambiente digital. O estelionato, uma forma específica de fraude, será abordado, assim como a invasão de privacidade, sob a perspectiva da Lei 12.737/2012, conhecida como Lei Carolina Dieckmann, que visa proteger as informações pessoais e dados dos usuários digitais contra invasões maliciosas. Dentro desse contexto, será explorada a dificuldade enfrentada pelas autoridades policiais na coleta de provas, devido à natureza desfavorável do ambiente para o rastreamento. Adicionalmente, o estudo discutirá a necessidade de perícias especializadas e a figura da produção antecipada de provas.

PALAVRAS CHAVE: Crimes cibernéticos. Internet. Ambiente virtual. Meios eletrônicos.

1 – INTRODUÇÃO

O presente estudo explana sobre o surgimento de novos delitos em decorrência do uso da internet, bem como a necessidade do Direito em acompanhar as mudanças

advindas da evolução tecnológica. Frente a isto, os crimes digitais serão abordados no contexto da influência da informática no Direito Penal e da necessidade de adaptação do direito à nova realidade tecnológica da sociedade contemporânea.

A análise sobre a sociedade contemporânea e o impacto da tecnologia da informação é bastante pertinente. De fato, a internet revolucionou a maneira como nos comunicamos, trabalhamos e vivemos, mas este fenômeno também suscita diversas questões jurídicas, que são fundamentais para a regulação e proteção dos direitos dos usuários e da sociedade como um todo.

A promulgação da Lei 12.965/14, também conhecida como o “Marco Civil da Internet” no Brasil, foi um passo significativo para o reconhecimento e a tipificação de crimes cibernéticos. No entanto, a luta contra os crimes na internet vai além da mera tipificação penal e enfrenta vários desafios intrínsecos à natureza desses delitos, como a natureza transnacional, a velocidade de execução, a dificuldade na produção de provas, os bens jurídicos atingidos e a necessidade de peritos capacitados.

A legislação, com a Lei 12.737/12, foi um esforço para tipificar e combater crimes cibernéticos, mas a eficácia dessa legislação enfrenta desafios, pois há uma necessidade de atualização contínua para acompanhar a rápida evolução tecnológica e as novas formas de criminalidade que surgem e, a impunidade é um dos aspectos mais preocupantes, pois muitas vítimas não denunciam os crimes, seja por falta de fé no sistema judicial, medo de represálias, ou insuficiência de evidências. Isso solicita um fortalecimento do sistema de justiça criminal para garantir que os responsáveis sejam processados e punidos.

Em um contexto global, iniciativas como a Convenção de Budapeste sobre Cibercrime, adotada em 2001, estabelece um marco jurídico internacional para a cooperação entre os países em matéria de crimes cibernéticos, onde tal convenção visa harmonizar legislações e facilitar a troca de informações entre estados.

E, diante de um cenário global em que os crimes cibernéticos estão em ascensão, é essencial que todos os setores da sociedade — incluindo governos, empresas e cidadãos — se unam para enfrentar este fenômeno. A promoção de uma legislação eficaz, a capacitação de autoridades e a conscientização da população sobre seus direitos são etapas fundamentais na construção de um ambiente digital mais seguro e justo.

Assim, a escolha do tema sobre crimes cibernéticos é verdadeiramente significativa, especialmente ao considerar a crescente prevalência desse tipo de delito

e as suas repercussões na vida dos indivíduos e na sociedade como um todo, com isso, o presente estudo busca enfatizar a relevância jurídica e político-social desse fenômeno.

2 – CRIMES CIBERNÉTICOS

A evolução dos crimes de informática revela uma transformação significativa no perfil dos criminosos, bem como nas técnicas utilizadas. Na década de 1970, esses crimes eram frequentemente elaborados por especialistas que exploravam vulnerabilidades nos sistemas de segurança, especialmente em instituições financeiras (RAMOS, 2017, p. 05). No entanto, esse cenário mudou consideravelmente, principalmente em relação ao perfil dos criminosos, pois a transformação no perfil dos criminosos de informática e a evolução das técnicas de ataque são reflexos da crescente sofisticação e acessibilidade da tecnologia.

Conforme ressalta Corrêa (2008, p. 42): "a internet é um paraíso de informações, e, pelo fato de essas serem riqueza, inevitavelmente atraem o crime. Onde há riqueza, há crime". Diante de tal situação e na existência de previsão legal, nascem os chamados crimes cibernéticos, tipificados pela prática de delitos no ambiente virtual ou por intermédio deste (WENDT; JORGE, 2014).

Os primeiros relatos de delitos envolvendo tecnologias de informação começaram a surgir com o advento dos computadores e suas aplicações em diversos setores. Nesta época, ainda era muito limitado o acesso à internet, e as infrações eram geralmente relacionadas a sistemas de computadores isolados, como intrusões e fraudes internas em organizações (D'URSO, 2017, p. 01).

Apenas em 1997, em uma reunião do G-8 – organização intergovernamental composta por 8 países (Alemanha, Canadá, Estados Unidos, França, Itália, Japão, Reino Unido e Rússia) para discutir questões econômicas, políticas e sociais de relevância global – que surgiu um ponto de inflexão na forma como os países começaram a ver o impacto dos crimes cibernéticos. Neste encontro, a discussão convergiu para a necessidade de uma abordagem internacional coordenada para combater os crimes ocorrendo no mundo virtual e, a partir daí, o termo "cibercrime" começou a ser oficialmente utilizado para descrever crimes que, por sua natureza, ocorrem em ambientes digitais ou que têm a tecnologia como ferramenta principal (D'URSO, 2017, p. 01).

A introdução de tecnologias digitais e o acesso generalizado à internet revolucionaram não apenas a maneira como os indivíduos se comunicam e conduzem

seus negócios, mas também a forma como os crimes são cometidos, onde a diversidade de nomenclaturas para os "crimes cibernéticos" reflete a complexidade e a evolução desse fenômeno.

Existem diversas denominações utilizadas para se referir a prática dessas infrações penais, onde alguns autores as definem como “crimes digitais”, os quais podem ser definidos, de acordo com Cassanti (2016, p. 02), como delitos praticados através da internet e ainda acrescenta que os crimes digitais são:

Toda atividade onde um computador ou uma rede de computadores é utilizada como uma ferramenta, base de ataque ou como meio de crime é conhecido como cibercrime. Outros termos que se referem a essa atividade são: crime informático, crimes eletrônicos, crime virtual ou crime digital (CASSANTI, 2014, p. 03).

Os crimes cibernéticos têm um impacto abrangente sobre uma variedade de bens jurídicos, tanto pessoais quanto patrimoniais. Esse fenômeno requer um atendimento multidisciplinar, incluindo legislação, educação, tecnologia e apoio psicológico, para garantir a segurança e a proteção dos indivíduos na era digital. Assim, a definição mais comum de crime cibernético é:

[...] aquele no qual um ou mais computador (es), equipamentos telemáticos ou dispositivos eletrônicos, interligados por meio de uma rede de comunicação, são utilizados, por um ou mais indivíduos, no cometimento de uma, ou mais conduta(s) criminalizada(s), ou são alvo(s) desta(s). O homem interagindo com uma máquina – retroalimentando-a com informações por meio de mensagens – através de uma rede de computadores (cibernética) interligados (ciberespaço), agindo conforme uma conduta previamente criminalizada (Crime informático) estereotiparia um modelo de cibercrime (COLLI, 2010, p. 44).

O primeiro passo dado no combate a esses delitos, foi a promulgação da lei 12.737/12, conhecida como Lei Carolina Dieckmann que, além da tipificação dos novos crimes oriundos da influência da evolução tecnológica, outras questões, diretamente afetadas pelas particularidades características dos crimes cibernéticos, merecem especial discussão, como a maneira e o ponto de desenvolvimento em que estão as legislações internacionais em matéria penal cibernética (RAMOS, 2017, p. 06).

O doutrinador Rossini (2004, p. 110), salienta que:

[...] o conceito de “delito informático” poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança Informática, que tem por elementos a integridade, disponibilidade a confidencialidade(ROSSINI, 2004, p. 110).

Esses delitos se perpetuam rapidamente em uma velocidade e novidade, atingindo os bens jurídicos com peculiaridades que dificultam a investigação criminal e a produção de provas. Todavia, os crimes cibernéticos dispõem de computadores, redes de computadores ou dispositivos eletrônicos conectados para realizar ações delituosas, no qual geram prejuízos a indivíduos ou patrimônios, através de extorsão de recursos financeiros, estresse emocional ou danos à reputação de vítimas expostas na Internet (SOARES, 2022, p. 12).

Entretanto, diante desse cenário, caberá ao novo profissional do Direito o papel de assegurar a proteção de diversos direitos como o de privacidade, a propriedade intelectual, a imagem, segurança da informação, direitos autorais e recebimento de royalties, processos contra hackers, por isso a importância de que seja o Direito Digital estudado profundamente a fim de que possa atender as novas necessidades advindas do ambiente virtual, cujo qual traz uma interligação que atinge empresas, pessoas, instituições e governos (PINHEIRO, 2013, p. 72).

Conforme Pinheiro (2013, p. 73): “não há um Direito da Internet, assim como não há um Direito Televisivo ou radiofônico, mas sim pontos específicos a serem analisados e regulamentados”. E, conforme enfatiza Marcelo Crespo (2011, p. 39), o direito da informática não se trata de um novo e específico ramo do Direito, mas sim uma nova interpretação jurídica relacionada a um novo momento de informação.

Assim, no cenário atual, a conscientização e a educação sobre segurança digital são essenciais para proteger indivíduos e organizações contra crimes cibernéticos, onde a vigilância contínua e a adaptação às novas ameaças são fundamentais para enfrentar esse desafio em constante evolução.

2.1 Da classificação e tipicidade dos crimes cibernéticos

A classificação dos crimes cibernéticos é essencial para a compreensão de suas nuances e implicações jurídicas. A divisão em categorias como crimes cibernéticos próprios, impróprios, mistos e mediatos ou indiretos permite uma análise mais detalhada e estruturada. São eles:

A) Crimes Cibernéticos Próprios: são aqueles cuja prática se dá exclusivamente no ambiente virtual. Nesses casos, a infração não poderia ocorrer se não houvesse a tecnologia da informação. Exemplos incluem o acesso não autorizado a sistemas de computador para roubar dados ou causar danos; programas maliciosos criados para

infectar sistemas, roubar informações ou danificar dispositivos; e-mails ou mensagens falsas projetadas para enganar usuários e coletar informações pessoais e financeiras.

Ao contrário dos crimes cibernéticos impróprios, que envolvem o uso da tecnologia como instrumento para a prática de crimes tradicionais, os crimes cibernéticos próprios têm como objeto a infração direta a bens jurídicos relacionados à tecnologia, tais como dados eletrônicos, sistemas informatizados e outros recursos tecnológicos (SOUZA; OLIVEIRA, 2021, p. 10).

Os artigos 313-A e 313-B do Código Penal Brasileiro tratam de crimes relacionados à manipulação de dados e informações informáticas com a conotação de abuso de poder por parte de funcionário público (BRASIL, 1940). Ademais, a interceptação ilegal de comunicações específicas via dispositivos eletrônicos é um crime cibernético próprio que pode causar sérios prejuízos à privacidade e à segurança das informações. A Lei nº 9.296/1996, que regulamenta a interceptação de comunicações telefônicas e de dados, aborda essa questão.

B) Crimes Cibernéticos Impróprios: são aqueles que, apesar de ocorrerem em um ambiente virtual, têm sua gênese em delitos que poderiam ser praticados fora do meio digital, isso significa que a infração tem uma tipificação legal que não depende da tecnologia. Exemplos incluem calúnia, difamação e estelionato.

Os crimes cibernéticos impróprios, também chamados de tradicionais em ambiente virtual, são aqueles em que a tecnologia é utilizada como instrumento para a prática de crimes já tipificados na legislação penal, tais como estelionato, falsidade ideológica, pornografia infantil, entre outros (ROSA, 2017, p. 67).

C) Crimes Cibernéticos Mistos: têm características tanto de delitos próprios quanto impróprios e podem ocorrer em situações em que as tecnologias digitais desempenham um papel crucial, mas não exclusivo. Exemplos incluem: Roubo de Identidade e fraudes com Cartões de Crédito. Conforme salienta Rossini (2004, p. 10), os crimes informáticos mistos são aqueles “em que o computador é mera ferramenta para a ofensa a outros bens jurídicos que não exclusivamente os do sistema informático”.

D) Crimes Cibernéticos Mediatos ou Indiretos: são aqueles que, mesmo não sendo tradicionalmente considerados crimes cibernéticos, têm a tecnologia como um meio facilitador ou vetor. Neste caso, o crime básico é potencializado pelo uso da internet ou das tecnologias digitais. Exemplos incluem: terrorismo e tráfico de drogas. De acordo com Vianna (2013) apud Lopes (2024, p. 11): “é o delito-fim não informático que herdou esta característica do delito-meio informático realizado para possibilitar a sua consumação.”

A categorização dos crimes cibernéticos em próprios, impróprios, mistos e mediatos é útil não apenas para fins acadêmicos, mas também para o desenvolvimento de políticas públicas e estratégias de combate a esses delitos. Compreender a natureza jurídica dos crimes cibernéticos e suas diferentes manifestações é fundamental para a elaboração de legislações adequadas e a implementação de medidas de segurança efetivas. Diante da constante evolução tecnológica, essas classificações precisam ser constantemente revisitadas e adaptadas para lidar com novas formas de criminalidade no ambiente digital.

2.2 Crimes cometidos por meio eletrônico

Sandro D'Amaro Nogueira (2009, p. 13), em sua análise sobre crimes cometidos por meio eletrônico, destaca a amplitude e diversidade dos delitos que podem ser perpetrados na era digital. A seguir, segue os principais tipos de crimes eletrônicos, suas características e as formas de execução:

1. Crimes Contra a Honra:

- Injúria: Consiste em ofender a dignidade ou o decoro de uma pessoa de forma direta. Exemplos incluem xingamentos e ofensas em redes sociais.

- Calúnia: Atribui falsamente a alguém a prática de um crime, difamando a sua imagem. Pode ocorrer, por exemplo, através de postagens em blogs ou redes sociais que afirmem que uma pessoa cometeu um crime que, na realidade, não ocorreu.

- Difamação: Consiste na propagação de informações falsas que denigram a imagem ou a reputação de uma pessoa. Tal prática é comum em comentários e compartilhamentos em plataformas digitais (GILABERTE, 2019, p. 10).

2. Furtos e Estelionatos:

- Furtos Eletrônicos: Envolvem a subtração de bens ou valores por meios digitais. Isso pode incluir o acesso não autorizado a contas bancárias para transferências de dinheiro.

- Estelionato: Utilização de fraudes online, como criar sites falsos para enganar usuários e obter informações pessoais ou financeiras (LOPES, 2023, p. 11).

3. Fraudes com Cartões de Crédito:

- O roubo de informações de cartões de crédito por meio de malware, phishing ou violações de segurança de dados é um crime comum. Os criminosos podem fazer compras não autorizadas ou vender as informações a terceiros (LOPES, 2023, p. 11).

4. Desvio de Dinheiro de Contas Bancárias:

- Refere-se ao acesso não autorizado às contas bancárias de uma pessoa ou empresa, geralmente realizado por meio de técnicas de engenharia social ou hacking. Isso pode resultar na transferência ilegal de fundos (LOPES, 2023, p. 12).

5. Interceptação de Comunicações:

- Técnicas que permitem a captura de mensagens eletrônicas, como emails e mensagens instantâneas, visando a obtenção de informações privadas ou sensíveis (NOGUEIRA, 2009, p. 08).

6. Modificações de Dados:

- Inclui a alteração de informações contidas em sistemas computacionais, que pode impactar empresas e indivíduos, resultando em prejuízos financeiros ou danos à reputação.

7. Difusão de Pornografia Infantil:

- A disseminação de conteúdo pornográfico envolvendo menores de idade é um crime severamente punido pela lei e tem crescido com o uso da internet e das redes sociais.

8. Terrorismo:

- O uso de tecnologia para a propagação de ideologias extremistas ou para a execução de ataques terroristas, incluindo recrutamento e financiamento de atividades terroristas através de plataformas digitais (NOGUEIRA, 2009, p. 08).

Os crimes eletrônicos são complexos e muito variados, refletindo a evolução da tecnologia e a capacidade dos criminosos de explorar vulnerabilidades no meio digital. Para combater eficazmente esses delitos, é fundamental que haja uma colaboração entre as autoridades, especialistas em segurança da informação e a sociedade civil. A educação e a conscientização sobre segurança digital são essenciais para minimizar os riscos e proteger indivíduos e instituições contra esses crimes. A legislação também deve ser continuamente adaptada para acompanhar a rápida evolução das táticas e tecnologias utilizadas por criminosos.

2.3 Legislação nacional frente aos crimes cibernéticos

O crescimento acelerado da internet e dos crimes virtuais tem desafiado o sistema jurídico brasileiro, onde as leis relacionadas a crimes virtuais evoluíram ao longo do tempo, mas ainda existem lacunas que podem ser exploradas, destacando-se o

Estatuto da Criança e do Adolescente (ECA), com a Lei nº 12.037, de 2009, que fez alterações significativas, incluindo penalizações para a produção, distribuição e posse de pornografia infantil, mesmo que esta ocorra virtualmente, sendo uma importante mudança para adaptar as leis existentes à fragilidade e nova realidade da internet.

A fragilidade da internet pode ser atribuída a vários fatores, incluindo sua complexidade tecnológica, já que envolve sistemas intrincados, servidores e dispositivos, o que gera múltiplas oportunidades de risco. O acelerado e contínuo surgimento de novas tecnologias frequentemente ultrapassa a capacidade de adotar medidas de segurança mais eficazes. Essa vulnerabilidade é uma consequência natural da complexidade e da interconexão global da internet. A rápida evolução tecnológica, somada à ausência de padrões de segurança universais, favorece a ocorrência de ameaças cibernéticas. Além disso, a ampla dependência da internet para diversas atividades, que vão desde a comunicação até transações financeiras, aumenta a probabilidade de ataques virtuais (GUIMARÃES, 2024, p. 16).

Os crimes cibernéticos têm repercussões legais consideráveis, especialmente no Brasil, demandando respostas abrangentes e adaptativas das autoridades e do sistema jurídico do país. As leis relacionadas à cibercriminalidade no Brasil estão em constante atualização para acompanhar o avanço acelerado das tecnologias digitais e as novas modalidades de atividades ilícitas no ambiente virtual. A principal área impactada é a legislação penal, que conta com algumas normas específicas para crimes cibernéticos, como a Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, a qual foi a pioneira em tratar penalmente os crimes cibernéticos, tipificando delitos como a invasão de dispositivos computacionais e o acesso não autorizado a dados (GUIMARÃES, 2024, p. 23).

De acordo com Silva, as leis tiveram que se atualizar com o avanço tecnológico (SILVA, 2003, p 28):

O aparecimento da Informática no meio social ocorreu de forma tão rápida e passou a exigir, com a mesma rapidez, soluções que o Direito não estava preparado para resolver. Com isso, a necessidade social aparenta estar desprovida da tutela do Direito e a busca ansiosa por regular a matéria pode provocar a criação de leis excessivas e desnecessárias.

Frente a isso, o Código Penal, em 2012, com a Lei nº 12.737, conhecida como a Lei Carolina Dieckmann, introduziu definições e penas específicas para crimes cibernéticos, como invasão de dispositivos eletrônicos. Isso mostrou um movimento em direção à regulamentação mais robusta de crimes virtuais. Nesse sentido, conforme Ramos (2017, p. 43):

Em decorrência de alguns episódios, em que em meados de 2011, ocorreram vários ataques de negação de serviço a sites do governo brasileiro que ficaram instáveis até sair do ar, ocasionando à atriz Carolina Dieckmann 36 fotos roubadas por hackers de seus arquivos pessoais e divulgadas na internet, que contribuíram para que as leis específicas sobre o tema fossem aprovadas em regime de urgência e com o objetivo de preencher as lacunas existentes no ordenamento, no que se refere aos crimes digitais, em 30/11/2012, foram sancionadas e promulgadas as leis 12.735, que trata da necessidade de instalação de órgãos investigativos especializados, e a lei 12.737, pela qual foram incluídos no Código Penal Brasileiro o tipo penal invasão de dispositivo informático (Art. 154-A) e a regra da ação penal para esse crime (Art. 154-B), conforme se extrai do Código Penal Brasileiro.

Ademais, vale ressaltar alguns pontos relevantes sobre a lei sancionada, 12.735/2012, onde tal lei foi fundamental na criação de órgãos investigativos especializados para tratar de crimes digitais, reconhecendo a necessidade de uma abordagem específica para esses delitos, além de introduzir importantes alterações no Código Penal Brasileiro, incluindo, além dos supra citados, o artigo 266, cujo texto foi revisado, incluindo interrupção ou perturbação de serviços relacionados à tecnologia da informação, refletindo o impacto crescente da tecnologia no cotidiano e a necessidade de proteger esses serviços; artigo 298, que incluiu cartões de crédito e débito como documentos particulares, ampliando a proteção contra fraudes e falsificações, reconhecendo a importância desses instrumentos na vida financeira moderna.

Assim, com a evolução das legislações brasileiras em relação aos crimes cibernéticos, diversas condutas passaram a ser punidas, entre elas destacam-se: Uso não autorizado de dados de cartões de crédito e débito (Artigo 155-A do Código Penal); Invasão de dispositivos eletrônicos (Artigo 154-A do Código Penal); Produção, oferta e venda de programas que permitem invasão (Artigo 285-B do Código Penal); Obtenção de informações sigilosas (Artigo 153 do Código Penal); Violação de comunicações eletrônicas (Artigo 151 do Código Penal).

Essas legislações demonstram um esforço para se adaptar às novas realidades trazidas pela tecnologia e fornecer mecanismos adequados para punir delitos associados à internet. No entanto, ainda existem desafios na aplicação eficaz dessas leis, incluindo a constante evolução das tecnologias e os métodos de perpetradores.

Em uma sucinta análise sobre os novos tipos penais criados com o advento da lei 12.737, Pinheiro (2013, p. 314) afirma que:

Ainda, receberá as mesmas penas da invasão aquele que instala uma vulnerabilidade em um sistema de informação para obter vantagem indevida, por exemplo, um backdoor ou uma configuração para que algumas portas de comunicação à internet fiquem sempre abertas. O usuário de gadgets e dispositivos informáticos comuns estão protegidos contra hackers e pessoas mal intencionadas que abusam de confiança ou buscam intencionalmente devassar dispositivo para se apropriar de dados do computador ou prejudicar o seu proprietário, com a exclusão ou alteração de dados, para que fiquem imprestáveis, ou ainda, informações íntimas e privadas, como fotos, documentos e vídeos. As empresas possuem maior proteção jurídica contra a espionagem digital, pois a obtenção de segredos comerciais e ou informações sigilosas definidas por lei agora também se enquadram na lei.

Em relação ao sujeito ativo dos crimes previstos nesta lei, pode-se afirmar que estamos diante de um crime comum, pois pode ser praticado por qualquer pessoa. No entanto, o legislador não se manifestou a respeito do proprietário do dispositivo informático ao definir a conduta de invadir um dispositivo alheio. Isso implica que a ação de um indivíduo, proprietário de uma lan house ou cyber café, que acesse indevidamente os dados de um usuário que utilizou sua máquina, será considerada atípica. O mesmo ocorrerá com o empregador que acessar e-mails pessoais do empregado compreendidos em seu computador de trabalho (VIANA; MACHADO, 2013, p. 94).

A crítica apresentada pelos respeitados autores Túlio Viana e Felipe Machado (2013, p.95) é pertinente ao afirmar que o bem a ser protegido deve ser a inviolabilidade dos dados, independentemente de quem seja o proprietário do dispositivo. A situação se torna mais complexa pelo fato de que não é possível realizar uma interpretação extensiva da conduta, uma vez que o Direito Penal brasileiro proíbe a analogia in malam partem, respeitando assim o princípio constitucional da legalidade, onde a solução para essa lacuna somente poderá ser encontrada por meio de uma nova legislação.

Quanto aos sujeitos passivos, estes podem ser tanto pessoas físicas quanto jurídicas que detêm dados informáticos, desde que não sejam as proprietárias do sistema computacional. A tipificação da conduta se dá com a ação de invadir e instalar, sendo que no segundo caso se refere à instalação de uma vulnerabilidade.

Esse crime é previsto exclusivamente na modalidade dolosa, ou seja, o agente deve estar ciente e ter a intenção de cometer o delito, sendo impossível a configuração da modalidade culposa e, em relação à temporalidade do crime, o artigo 4º do Código Penal adota a teoria da atividade, o que implica que a invasão ao dispositivo informático é considerada consumada no momento em que o comando para acesso não autorizado é emitido (VIANA; MACHADO, 2013. P. 94).

Nota-se que a aprovação de Projetos de Lei que visam proteger os usuários da internet é uma resposta clara à crescente preocupação com a vulnerabilidade das pessoas nesse ambiente digital, onde um dos principais objetivos dessas leis é oferecer uma estrutura de proteção que garanta a segurança, os direitos e a privacidade dos internautas. Contudo, embora existam leis que tratam de crimes virtuais, a aplicação delas enfrenta desafios, como a dificuldade de rastreamento de criminosos, a proteção da privacidade dos indivíduos e a necessidade de cooperação internacional para lidar com crimes que transcendem fronteiras.

A aprovação de legislações que buscam proteger os usuários da internet reflete uma preocupação crescente em relação à vulnerabilidade das pessoas nesse meio digital. Um dos objetivos principais dessas leis é fornecer uma estrutura de proteção que assegure a segurança, os direitos e a privacidade dos internautas. No entanto, mesmo com a existência de leis voltadas para crimes virtuais, sua aplicação encontra obstáculos, como a dificuldade de identificar os criminosos, a necessidade de proteger a privacidade das pessoas e a urgência de cooperação internacional para lidar com crimes que ultrapassam fronteiras (GUIMARÃES, 2024, p. 09).

Assim, a adequação legislativa frente aos crimes cibernéticos é um tema de grande relevância, principalmente na era digital em que vivemos. Os crimes cibernéticos incluem uma variedade de delitos, como fraudes online, roubo de dados, invasões de sistemas, entre outros e, para lidar com esses desafios, muitos países têm buscado atualizar e criar legislações específicas.

2.4 Visão geral da legislação atual sobre crimes virtuais no Brasil

A legislação brasileira enfrenta desafios constantes ao tentar se adaptar ao rápido avanço da tecnologia e, por consequência, ao aumento dos crimes cibernéticos. Essa situação se torna ainda mais complicada quando consideramos a natureza desses delitos, que muitas vezes transcendem as fronteiras de um país, exigindo uma atuação legal que transcenda fronteiras. Lira e Salgado (2021) destacam a relevância do princípio da extraterritorialidade, especialmente no contexto digital, o que requer uma atualização do direito penal nacional para abranger essa nova realidade.

A Lei 12.965/2014, conhecida como Marco Civil da Internet, foi um avanço significativo na regulamentação da internet no Brasil, especialmente no que diz respeito ao direito à privacidade online. No entanto, Calgaroto (2021) enfatiza que, apesar das inovações introduzidas por essa legislação, ainda persistem desafios em relação à responsabilização civil e à proteção efetiva dos direitos dos usuários.

Outra questão que se destaca é a falta de legislação específica para certos crimes cibernéticos, especialmente aqueles que ferem a honra das pessoas. Stephane e De Andrade (2022) abordam essa lacuna e enfatizam a necessidade de uma atuação mais forte por parte do Estado para salvaguardar a dignidade das vítimas.

Entretanto, é importante mencionar os esforços recentes para modernizar a legislação. Gomes e Medrado (2023) discutem a Lei 14.155 de 2021, que aborda especificamente o crime de estelionato virtual, evidenciando um movimento legislativo que busca respostas mais adequadas aos desafios do ambiente digital.

Theuherz e Santos (2023) abordam a questão dos crimes virtuais de maneira mais abrangente, ressaltando a necessidade de uma legislação específica, atualizada e eficiente que possa combater a crescente criminalidade cibernética, a qual ameaça tanto indivíduos quanto instituições.

Veiga e Da Silveira (2022) analisam a (in)eficácia da lei conhecida como "Lei Carolina Dieckmann", destacando a importância de constantes revisões e atualizações na legislação, juntamente com a implementação efetiva das normas já existentes.

Nogueira e Nolasco (2022) argumentam que os crimes cibernéticos representam um grande desafio para o Direito, pois sua natureza e métodos de execução são diferentes dos crimes convencionais, exigindo uma abordagem jurídica que seja diferenciada e mais compatível com a realidade virtual.

Bonini et al. (2018) enfatizam a necessidade de um entendimento claro e aprofundado sobre os crimes cibernéticos para que a legislação seja aplicada de forma eficaz, garantindo assim a penalização adequada e a proteção das vítimas.

Por fim, a coleta de provas em processos penais relacionados a crimes virtuais representa um dos principais desafios para o sistema judiciário brasileiro. Santana (2019) ressalta que a natureza passageira das evidências digitais requer uma abordagem técnica e especializada, a fim de assegurar a justiça e a adequada aplicação da legislação.

3 LIMITAÇÕES E LACUNAS

O ambiente digital, apesar de trazer diversas vantagens, também se mostrou um espaço propício para a prática de ações criminosas. Conforme apontam Lopes e Lopes (2023), a legislação brasileira enfrenta diversos obstáculos na tentativa de acompanhar essa evolução. Os autores enfatizam que as normas em vigor ainda não conseguem

contemplar a totalidade dos crimes que podem ocorrer no meio virtual, resultando em lacunas significativas no sistema jurídico do Brasil.

Calgarato (2021) reflete sobre a privacidade na internet e suas consequências. Ele observa que, apesar dos avanços trazidos pelo Marco Civil da Internet, a responsabilização civil em casos de violações ainda se encontra em uma situação instável e, embora essa legislação tenha buscado modernizar e adequar o direito à era digital, ela não resolveu todas as questões relacionadas aos delitos virtuais.

Uma lacuna importante na legislação diz respeito à coleta de provas em processos penais relacionados a crimes cibernéticos. Santana (2019) aponta os obstáculos enfrentados na obtenção e validação de evidências neste tipo de crime, já que a natureza dinâmica e dispersa do ambiente digital torna desafiadora a identificação e a preservação de provas concretas.

Bonini et al. (2018) abordam os crimes cibernéticos de forma abrangente e ressaltam que a rapidez das inovações tecnológicas demanda uma constante atualização das leis. Muitas vezes, quando uma nova legislação é finalmente aprovada, os criminosos já criaram novas estratégias, tornando-as rapidamente obsoletas ou inadequadas.

Entre os crimes cibernéticos que têm se destacado está o estelionato virtual. Gomes e Medrado (2023) comentam sobre a recente Lei 14.155 de 2021, que aborda esse tipo de crime. Eles argumentam que, apesar de ser um progresso, a lei ainda permite múltiplas interpretações e não cobre todas as possíveis formas de cometimento desse delito.

As omissões na legislação também constituem uma preocupação, especialmente no que diz respeito aos crimes cibernéticos contra a honra. Stephane e De Andrade (2022) criticam a ausência de normas claras e específicas para essa categoria de crimes, o que torna o processo de responsabilização e punição mais complicado e, em muitos casos, ineficaz.

Nogueira e Nolasco (2022) abordam os desafios que o direito enfrenta em relação aos crimes cibernéticos. Eles destacam a necessidade de equilibrar as garantias individuais com a segurança coletiva, um dilema que a legislação vigente ainda não resolve de maneira satisfatória.

O Brasil, quando comparado a outros países, ainda tem um longo percurso a seguir no que diz respeito à eficácia de suas leis contra os crimes cibernéticos. Veiga e Da Silveira (2022) realizam uma análise crítica da Lei Carolina Dieckmann e sua

efetividade, concluindo que, embora represente um progresso, ainda existem muitas melhorias a serem feitas.

Por fim, a era digital suscitou um debate sobre o princípio da extraterritorialidade. Lira e Salgado (2021) investigam como os crimes cibernéticos podem ser perpetrados de qualquer parte do mundo, o que complica a definição de jurisdição e a aplicação de leis específicas. Dessa forma, a internacionalização dos delitos cibernéticos representa um desafio adicional para o sistema jurídico brasileiro.

Essas considerações mostram que, apesar dos esforços recentes para modernizar a legislação, ainda existem lacunas e limitações significativas a serem enfrentadas no contexto dos crimes cibernéticos no Brasil, já que as contínuas inovações e mudanças tecnológicas exigem uma resposta rápida e adequada do direito, um aspecto que ainda representa um desafio atualmente.

4 – CONCLUSÕES

Ao longo das discussões e análises, destaca-se a necessidade essencial de adaptar a legislação brasileira às demandas atuais que surgem na era digital. A propagação de informações, especialmente em um contexto globalizado e hiperconectado, traz não só oportunidades, mas também desafios significativos, particularmente no que diz respeito à disseminação de fake news e à ocorrência de crimes virtuais. A tensão entre proteger a sociedade dos riscos da desinformação e preservar direitos fundamentais, como a privacidade e a liberdade de expressão, ilustra a complexidade envolvida na tarefa de legislar em um campo tão dinâmico quanto o digital.

É fundamental que tanto legisladores quanto a sociedade civil continuem a trabalhar juntos para ajustar e criar novas leis que respondam a essa evolução tecnológica e, apesar das legislações existentes, muitos desafios permanecem, como a rapidez da tecnologia, uma vez que a legislação muitas vezes não acompanha a velocidade das inovações tecnológicas e novas modalidades de crimes; falta de capacitação, pois a aplicação da legislação requer profissionais capacitados, tanto em termos de investigação quanto no âmbito judicial; propostas de melhoria; atualização frequente das Leis, pois é fundamental que as legislações sejam constantemente atualizadas para enfrentar novas ameaças; investimento em capacitação, com treinamentos para policiais, juízes e advogados sobre as especificidades do direito digital; bem como acordos internacionais, com o intuito de cooperar com outros países para enfrentar crimes transnacionais e compartilhar informações eficazes.

A adequação legislativa frente aos crimes cibernéticos é um processo contínuo que requer a colaboração entre diferentes setores da sociedade, incluindo governos, instituições legais, empresas de tecnologia e os usuários, sendo essencial que os legisladores se mantenham atualizados e proativos para garantir a segurança no ambiente digital.

Em síntese, a questão dos crimes cibernéticos e da desinformação no Brasil é um campo em constante evolução que requer uma atenção especial do Direito. A interação entre tecnologia, sociedade e legislação deve ser harmonizada de modo a garantir uma internet segura, justa e livre para todos os seus usuários. A busca por esse equilíbrio, como demonstrado, é uma jornada contínua e essencial no cenário atual.

REFERÊNCIAS

- BONINI, L. M. *et al.* **Crimes Cibernéticos**. Diálogos Interdisciplinares, v. 7, n. 3, p. 223-236, 2018.
- CALGAROTO, C. **O direito à privacidade na internet: panorama, responsabilização civil e inovações do marco civil da internet (Lei nº 12.965/2014)**. Direito-Unisul Virtual, 2021. CAZAROTI, T. M. B.; PINHEIRO, E. F. **Crimes Cibernéticos**. TCC-Direito, 2021.
- CASSANTI, M. O. **Crimes Virtuais, Vítimas reais**. Rio de Janeiro: Brasport, 2014.
- COLLI, M. **Cibercrimes. Limites e perspectivas à investigação policial de crimes cibernéticos**. Juruá Editora, 2010.
- CORRÊA, G. T. **Aspectos jurídicos da internet**. Saraiva, 2008.
- D'URSO, L. A. F. **Cibercrime: perigo na internet**. Publicado em 2017. Disponível em: <<http://politica.estadao.com.br/blogs/faustomacedo/cibercrime-perigona-internet/>>. Acesso em: 20/11/2024.
- GILABERTE, Bruno. **Crimes Contra a Pessoa**. Editora Freitas Bastos 2º Ed, 2019.
- GOMES, W. M.; MEDRADO, L. C. **CRIMES CIBERNÉTICOS UMA PONDERAÇÃO SOBRE A LEI 14.155 DE 2021 APLICÁVEL AO CRIME DE ESTELIONATO VIRTUAL**. Revista Ibero-Americana de Humanidades, Ciências e Educação, v. 9, n. 9, p. 1870-1894, 2023.
- GUIMARÃES, P. V. **Criminalidade virtual: desafios do Direito Brasileiro face ao avanço dos crimes cibernéticos**. PUC Goiás: 2024. Disponível em: <<https://repositorio.pucgoias.edu.br/jspui/bitstream/123456789/7549/1/PEDRO%20VIN%20C3%84DCIUS%20GUIMAR%20C3%83ES.pdf>> Acesso em: 24/03/2025.
- LAKATOS, E. M.; MARCONI, M. de A. **Fundamentos de metodologia científica**. 5. ed. São Paulo: Atlas, 2003.

LIRA, C. C. D.; SALGADO, A. A. R. T. **A era digital e a prática de crimes cibernéticos: uma análise sobre o princípio da extraterritorialidade**. Criminalidade Na Era Digital, v. 58046, p. 68. 2021.

LOPES, A. S. **Estelionato virtual**. PUC: Goiás, 2023. Disponível em: <<https://repositorio.pucgoias.edu.br/jspui/bitstream/123456789/5630/1/A05%2005%20ARTIGO%20COMPLETO.pdf>> Acesso em: 10/12/2024.

LOPES, M. P.; LOPES, J. A. B. **CRIMES VIRTUAIS NO ORDENAMENTO JURÍDICO BRASILEIRO**. Revista Ibero-Americana de Humanidades, Ciências e Educação, v. 9, n. 8, p. 462-472, 2023.

MARTINS, G. A.; PINTO, R. L. **Manual para elaboração de trabalhos acadêmicos**. São Paulo: Atlas, 2001.

NOGUEIRA, F. M. S.; NOLASCO, L. G. **Crimes Cibernéticos Desafios Para O Direito**. Revista Jurídica Direito, Sociedade E Justiça, v. 9, n. 13, p. 133- 140, 2022.

PINHEIRO, P. P. **Direito Digital**. São Paulo: Editora Saraiva, 2013.

RAMOS, E. D. **Crimes Cibernéticos: análise evolutiva e legislação penal brasileira**. UFRJ: Rio de Janeiro, 2017.

ROSA, F. S. **Crimes Cibernéticos: aspectos penais e processuais**. São Paulo: JH Mizuno, 2017.

ROSSINI, A. E. S. **Informática Telemática e Direito Penal**. São Paulo: Memória Jurídica 2004.

SANTANA, D. R. [Graduação| Monografia] **Sistema de provas nos crimes virtuais: os desafios da instrução probatória em ações penais relativas aos crimes virtuais no Brasil**. Portal de Trabalhos Acadêmicos, v. 6, n. 1, 2019.

SILVA, P. S. **Direito e crime cibernético: análise da competência em razão do lugar no julgamento de ações penais**. Brasília: Vestnik, 2015. Disponível em: <<https://profmatheus.com/wp-content/uploads/2017/05/direito-crime>> Acesso em: 24/03/2025.

SOARES, M. L. P. **Crimes cibernéticos: a deficiência da legislação penal brasileirae os projetos de leis governamentais**. Universidade Potiguar: Natal/RN, 2022.

STEPHANE, T.; DE ANDRADE, G. H. A. **A Omissão Legislativa Do Estado Nos Crimes Cibernéticos Contra A Honra**. Praxis Jurídica, v. 6, n. 2, 2022. THEUHERZ, Nícolas Gava Baesso; SANTOS, Kaully Furiama. Crimes virtuais. Revista Mato-grossense de Direito, v. 1, n. 1, p. 146-160, 2023.

VEIGA, D. J. S.; DA SILVEIRA, D. P. Joselia Cristina Siqueira da Silva *et al.*. **O cibercrime no brasil: uma análise da (in) eficácia da lei carolina dieckmann**, International Journal of Development Research, v. 11, n. 01, p. 43466- 43469.

VIANA, T.; MACHADO, F. **Crimes informáticos**. Belo Horizonte: Fórum, 2013.

WENDT, E.; JORGE, H. V. N. **Crimes cibernéticos: ameaças e procedimentos de investigação**. 2ª Ed. Rio de Janeiro: Brasport, 2013.