UNILEÃO
CENTRO UNIVERSITÁRIO DOUTOR LEÃO SAMPAIO
CURSO DE GRADUAÇÃO EM DIREITO

MÁRIO ENZZO BEZERRA COSTA NOGUEIRA

A (IN)EFICÁCIA DA LEGISLAÇÃO BRASILEIRA EM RELAÇÃO AOS CRIMES VIRTUAIS

JUAZEIRO DO NORTE-CE
2024

MÁRIO ENZZO BEZERRA COSTA NOGUEIRA

À (IN)EFICÁCIA DA LEGISLAÇÃO BRASILEIRA EM RELAÇÃO AOS CRIMES VIRTUAIS

Trabalho de Conclusão de Curso – *Artigo Científico*, apresentado à Coordenação do Curso de Graduação em Direito do Centro Universitário Doutor Leão Sampaio, em cumprimento às exigências para a obtenção do grau de Bacharel.

Orientador: Esp. Francisco Gledison de Lima Araújo

JUAZEIRO DO NORTE-CE
2024

MARIO ENZZO BEZERRA COSTA NOGUEIRA

À (IN)EFICÁCIA DA LEGISLAÇÃO BRASILEIRA EM RELAÇÃO AOS CRIMES VIRTUAIS

Este exemplar corresponde à redação final aprovada do Trabalho de Conclusão de Curso de MARIO ENZZO BEZERRA COSTA NOGUEIRA.

Data da Apresentação 09/12/2024

BANCA EXAMINADORA

Orientador: FRANCISCO GLEDISON LIMA ARAÚJO

Membro: JOSÉ BOAVENTURA FILHO

Membro: LUIS JOSÉ TENÓRIO BRITTO

JUAZEIRO DO NORTE-CE
2024

À (IN)EFICÁCIA DA LEGISLAÇÃO BRASILEIRA EM RELAÇÃO AOS CRIMES VIRTUAIS

Mario Enzzo Bezerra Costa Nogueira[1]
Francisco Gledison Lima Araújo[2]

RESUMO

O presente trabalho tem como objetivo analisar as limitações das leis no combate aos crimes virtuais no Brasil, investigar possíveis lacunas e propor soluções. A metodologia utilizada foi a pesquisa qualitativa, com análise de documentos legais e pesquisa bibliográfica, fundamentando-se em doutrinas, dissertações, artigos e material disponível na internet. Os principais resultados revelam que a Lei Carolina Dieckmann introduziu a tipificação da "invasão de dispositivo informático" no Código Penal, visando proteger a privacidade dos usuários, enquanto o Marco Civil da Internet estabelece princípios para a utilização da internet, promovendo a proteção de dados e a responsabilidade dos provedores. No entanto, ambas as leis apresentam lacunas, como a falta de clareza em definições e a necessidade de atualização frente a evolução tecnológica. As conclusões indicam que, para uma proteção mais eficaz dos cidadãos no ambiente digital, é imprescindível uma revisão e complementação das legislações existentes.

Palavras Chave: crimes virtuais; legislação brasileira; proteção do usuário.

1 INTRODUÇÃO

Dado o crescimento do uso da internet no Brasil, percebe-se que os sistemas jurídicos não estão conseguindo acompanhar o ritmo dos desenvolvimentos digitais. Os benefícios trazidos pela internet são evidentes, mas os maliciosos também surgiram, principalmente em relação aos criminosos que a utilizam como ferramenta para atividades delitivas. Como consequência, um número crescente de pessoas está sendo afetado no ambiente digital, onde sofrem insultos ou ataques que causam algum prejuízo. À medida que a internet avança, a legislação deve ser aprimorada para acompanhar a sua evolução. Os crimes virtuais existem em formas diferentes; algumas condutas praticadas pela internet são penalmente consideradas típicas, mas outras são vistas como atípicas. Ou melhor, estas não seriam reconhecidas como crime devido à escassa legislação sobre comportamentos que utilizam a informática, em

[1]Mário Enzzo Bezerra Costa Nogueira, Graduando do Curso de Direito do Centro Universitário Doutor Leão Sampaio/mario_enzzo@hotmail.com
[2]Francisco Gledison Lima Araújo, Professor do Centro Universitário Doutor Leão Sampaio/UNILEÃO, Especialista em Direito, novas tecnologias e inteligência artificial, Esp. direito Público e Constitucional

conjunto com o Princípio da Reserva Legal, um pilar do Direito Penal, segundo o qual não existe crime ou pena sem prévia determinação legal.

A Lei 12.737/12, também popularmente conhecida como Lei Carolina Dieckmann, surgiu após o vazamento de fotos íntimas da atriz, incluindo no Código Penal uma previsão legal, ou seja, uma classificação criminal chamada "invasão de dispositivo informático". Logo depois, em 2014, foi promulgada a Lei 12.965, nomeada "Marco Civil da Internet", popularmente conhecida como a Constituição da Internet Brasileira. Essa lei tem como objetivo principal regular a relação entre as empresas que oferecem produtos ou serviços relacionados à internet e seus usuários no território nacional.

A formulação deste trabalho é complementar as lacunas do sistema jurídico do nosso país em relação aos cybercrimes e definir claramente os direitos, proteções e responsabilidades dos meios de comunicação digitais. Todavia, embora pareça ser eficiente no tratamento dos direitos dos usuários, ainda apresenta algumas deficiências. Diante disso, o presente trabalho surgiu da seguinte problemática: por que a legislação brasileira atual, como as Leis 12.737/12 e 12.965/14, ainda é ineficaz no combate e na prevenção dos crimes virtuais? Dessa forma, o escopo geral deste estudo é analisar as limitações da legislação brasileira em relação aos crimes virtuais, com foco nas Leis 12.737/12 (Lei Carolina Dieckmann) e 12.965/14 (Marco Civil da Internet). Seu objetivo específico é discutir o conceito e a classificação dos crimes virtuais, explicando a diferença entre crime cibernético próprio e impróprio; identificar e descrever alguns dos crimes cibernéticos mais comuns no Brasil; e discutir algumas limitações das Leis 12.965/14 (Marco Civil da Internet) e 12.737/12 (Lei Carolina Dieckmann). Diante disso, o estudo defende a necessidade de analisar criticamente a legislação atual e propor possíveis melhorias para garantir uma maior eficácia no combate aos crimes virtuais, protegendo assim os direitos e a segurança dos cidadãos no ambiente digital.

2 DESENVOLVIMENTO

2.1 METODOLOGIA

O método de pesquisa utilizado foi o qualitativo, envolvendo análise de documentos legais, onde a análise dos dados ocorreu por meio de pesquisa bibliográfica, sendo aquela que possui como objetivo o fornecimento de fundamentação teórica, visto que teve como base material já publicado. Logo, o presente trabalho possui como base, doutrina, dissertações,

artigos, bem como material disponibilizado na Internet. O estudo em questão utilizará, a priori, o material disponibilizado no meio eletrônico, como a plataforma Google Acadêmico, na base de dados SciELO - Brasil, bem como, livros, legislações, artigos e jurisprudência.

2.2 REFERENCIAL TEÓRICO

2.2.1 Crimes cibernéticos

Primeiramente, vale ressaltar que internet tem se expandido bastante, assim como o número de seus usuários. Atualmente, é considerada o maior sistema de comunidade global, devido aos vários recursos que apresentam para facilitar a vida de seus usuários. A busca por informações, relacionamentos, entretenimento, transações bancárias, são umas das principais atividades desenvolvidas. Entretanto, determinados usuários usufruem de forma prejudicial, assim praticando os chamados crimes virtuais. Todavia, não há nomes específicos para tais crimes; portanto, estes crimes são também conhecidos como cybercrimes, crime informático, crime tecnológico, crimes eletrônicos, crime digital, entre outros. Nessa perspectiva, Silva afirma:

> […] que não há uma nomenclatura sedimentada pelos doutrinadores acerca do conceito de crime cibernético. De uma forma ou de outra o que muda é só o nome atribuído a esses crimes, posto que devem ser notados o uso de dispositivos informáticos, a rede de transmissão de dados para delinquir, o bem jurídico lesado, e ainda deve a conduta ser típica, antijurídica e culpável. (Da Silva, 2015, p.39).

Com relação à Maia os crimes cibernéticos são definidos como:

> Uma definição bem completa para o crime de informática é a que o caracteriza como uma conduta atentatória ao estado natural dos dados e recursos oferecidos pelos sistemas de processamento de dados, e pela compilação, armazenamento, e transmissão dos dados. O crime de informática, desse modo, é aquele procedimento que ataca os dados armazenados, compilados, transmissíveis, ou em transmissão (Maia, 2017, p. 31).

Por tanto, conforme os autores citados, o crime informático nada mais é do que qualquer ato realizado por meio de computadores, onde os meios informáticos são objeto do crime. A infração está relacionada ao fenômeno do crime de informação, que qualquer pessoa que viole direitos fundamentais, cometerá o delito. Assim sendo, no mesmo pensamento, Cassanti enfatiza:

> Toda atividade em que um computador ou uma rede de computadores é utilizada como uma ferramenta, base de ataque ou como meio de crime é conhecido como cibe crime. Outros termos que se referem a essa atividade são: crime informático, crimes eletrônicos, crime virtual ou crime digital. (Cassanti, 2014, p. 3).

A conclusão que se tem então, é que o crime virtual é um típico crime ilegal. Satisfaz os pré-requisitos de um crime ou contravenção penal, consciente, que pode ser cometido por pessoas físicas ou jurídicas por meio de tecnologia da informação.

2.2.2 Crimes cibernéticos próprios e impróprios

A classificação amplamente utilizada, e que será adotada neste texto, é a proposta por Hervé Croze e Yves Bismuth, que dividem os crimes de informática em duas modalidades.

> [..] Os crimes próprios: diz respeito aos atos dirigidos contra o sistema de informática, subdivididos em: atos contra o computador (ou seja, contra o próprio material informático, o computador propriamente dito e seus componentes e suportes como os disquetes e fitas magnéticas); e atos contra os dados ou programas de computador (contra as informações do computador, pela cópia não autorizada das informações, alteração ou destruição de dados dos suportes) (Texeira, 2024. p. 592).

Portanto os crimes próprios são aqueles que só podem ser cometidos com o uso da informática; sem ela, a execução e a consumação do delito se tornam impossíveis. Esses tipos penais são relativamente novos, surgindo com o avanço e a popularização da tecnologia da informação, sendo a própria informática o bem protegido pela legislação penal.

São exemplos:

Hacking (invasão de sistemas): Quando um criminoso acessa sistemas de computador sem autorização, geralmente com o objetivo de roubar informações, danificar dados ou obter vantagens ilícitas.

Phishing: Quando o criminoso cria um site ou e-mail falso para enganar as vítimas e roubar suas informações pessoais, como senhas e números de cartão de crédito.

Malware: Programas maliciosos criados para danificar ou acessar de forma clandestina sistemas e dados, como vírus, worms e trojans.

Já os crimes impróprios conforme definição abaixo se referem a delitos já estabelecidos na legislação penal que não se configuram precisamente como crimes de informática. Esses atos são cometidos por meio de sistemas de informática, ou seja, qualquer crime que utilize a tecnologia da informação como ferramenta para sua execução.

> [..] Crimes impróprios: são aqueles praticados de várias formas, inclusive mediante o uso da informática. Logo, o computador é um meio, ou o instrumento, utilizado para a execução do crime. São crimes que já têm proteção por nossa legislação penal, como, por exemplo: contra o patrimônio, o estelionato; contra a honra, a calúnia; contra a liberdade individual, a violação da intimidade, da correspondência e da liberdade de comunicação; contra a propriedade imaterial, a violação de marcas, patentes e direitos autorais (inclusive o software, que, por determinação legal, Lei n. 9.609/98, é considerado como criação intelectual) (Brasil, 1998).

São exemplos:

Fraude financeira: Uma pessoa pode utilizar um computador ou aplicativo para realizar uma fraude bancária, como transferências indevidas ou roubo de valores de contas bancárias.

Difamação online (Cyberbullying): Quando alguém espalha mentiras, boatos ou realiza ataques contra a reputação de outra pessoa nas redes sociais ou em fóruns.

Venda de produtos falsificados: Usar plataformas de e-commerce para vender produtos ilegais ou falsificados, como roupas, eletrônicos ou medicamentos

2.2.3 Crimes contra o patrimônio em geral

Uma das modalidades de crime mais alarmantes, que pode atingir o patrimônio de pessoas físicas ou jurídicas, inclui delitos como furto, estelionato, dano e extorsão. Um exemplo conhecido é a transferência de dinheiro de contas de terceiros para contas controladas pelos criminosos. No sistema bancário, uma das fraudes mais comuns é o "salami slicing" (fatia de salame), onde pequenas quantias são retiradas de várias contas e enviadas para a conta do golpista. No passado, muitos desses crimes contavam com a colaboração interna de funcionários de instituições financeiras, que forneciam senhas de clientes aos criminosos. Além disso, a facilidade de abertura de contas bancárias no Brasil, utilizando documentos falsos, também facilita esse tipo de crime. (Texeira, 2024).

Quanto ao crime de dano, que envolve destruir ou inutilizar propriedade alheia, há discussões sobre a tangibilidade de elementos digitais, como bits. Se o Projeto de Lei n. 84/99 fosse aprovado, buscando criminalizar a criação e disseminação de vírus de computador, essa questão poderia ser resolvida, pois tais atos seriam considerados crimes de dano. O professor Edson Rodrigues, da USP, argumenta que um bit é um bem material, pois representa um estado físico em um dispositivo de armazenamento. (Texeira, 2024).

2.2.4 Crimes contra a honra, calúnia e difamação

São atos que denigrem a integridade moral das pessoas via calúnia, injúria ou difamação, utilizando-se da internet como instrumento de pulverizar as ofensas morais, que podem ocorrer por dizeres, fotos, imagens, desenhos, entre outros. Alguns infratores são motivados pela ampla oportunidade de permanecer anônimos online. Isso se deve à dinâmica constante das redes sociais e páginas na web, que permitem não apenas o acesso de qualquer pessoa, mas também a chance de se esconder por trás de pseudônimos.

O Código Penal brasileiro em seu Capítulo V, Título I da Parte Especial relata sobre:

> ‘Os Crimes Contra a Honra’’. Tem como garantia fundamental pela Constituição da República Federativa do Brasil, que em seu artigo 5.º, inciso X, fomentou que “são invioláveis a intimidade, a vida privada, a honra é a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.

Honra é, sem dúvida, um direito fundamental do ser humano, protegido constitucionalmente e penalmente. Segundo Nucci (2014, p. 3) honra “é a faculdade de apreciação ou o senso que se faz acerca da autoridade moral de uma pessoa, consistente na sua honestidade, no seu bom comportamento, na sua respeitabilidade no seio social, na sua correção moral”.

Desdobra-se em dois aspectos, o subjetivo e o objetivo conforme ensina Luís Regis Prado (2015, p. 764 – 765)

> A honra, do ponto de vista objetivo, seria a reputação que o indivíduo desfruta em determinado meio social, a estima que lhe é conferida; subjetivamente, a honra seria o sentimento da própria dignidade ou decoro. A calúnia e a difamação atingiriam a honra no sentido objetivo (reputação, estima social, bom nome); já a injúria ofenderia a honra subjetiva (dignidade, decoro).

A honra é um valor jurídico que deve ser preservado. Os crimes mais notórios contra a honra são a calúnia, a difamação e a injúria. Essas ações podem ser realizadas de diversas maneiras, inclusive através do mundo virtual. Nos dias de hoje, as redes sociais são onde mais frequentemente ocorrem esses tipos de ataques ofensivos, pois oferecem aos agressores a ilusão de que podem permanecer anônimos e impunes.

O dolo é um elemento subjetivo fundamental nos delitos contra a honra, podendo se manifestar de forma direta ou eventual. É imprescindível a vontade do agente em atingir a honra objetiva (calúnia e difamação) ou a honra subjetiva (injúria). Não está prevista, portanto, a responsabilidade culposa nesse delito.

Os crimes que violam a honra estão previstos no Código Penal em três modalidades: a calúnia (art. 138 CP), a difamação (art. 139 CP) e a injúria (art. 140 CP).

Destaque-se que, nos crimes contra a honra, se a conduta criminosa é cometida ou divulgada em quaisquer modalidades das redes sociais da rede mundial de computadores, aplica-se em triplo a pena, nos termos do § 2º do art. 141 do Código Penal, incluído pela Lei n. 13.964/2019.

2.3 LEGISLAÇÃO APLICÁVEL AOS CRIMES CIBERNÉTICOS

2.3.1 Analise da lei 12.737/2012 (lei Carolina Dieckmann)

Em 2011, a atriz Carolina Dieckmann teve sua intimidade violada após um grupo de hackers invadir seu computador pessoal e divulgar sem autorização 36 imagens íntimas pelas redes sociais. Além das fotos roubadas, a atriz chegou a receber ameaças e extorsões para evitar a exposição. O autuado foi indiciado por extorsão conforme o artigo 158 do Código Penal:

> Art. 158 - Constranger alguém, mediante violência ou grave ameaça, e com o intuito de obter para si ou para outrem indevida vantagem econômica, a fazer, tolerar que se faça ou deixar de fazer alguma coisa:
>
> Pena - reclusão, de quatro a dez anos, e multa.

Na época do crime, ainda não existia uma legislação específica que abrangesse esse tipo de delito. A atriz realizou uma grande campanha e, ao final, conseguiu que o congresso aprovasse a lei 12.737/12, em 30 de novembro de 2012, deu origem ao crime de invasão de aparelho informático, e inseriu no Código Penal o artigo 154-A, prevendo o crime. Esta foi a primeira lei a tratar de forma específica sobre os crimes virtuais, trazendo grande inovação e criando um novo tipo penal (Texeira, 2024).

> 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:
>
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa (Brasil, 2012).

A referida norma legal, ao longo dos anos, passou por diversas alterações, demonstrando a preocupação do legislador em acompanhar a evolução tecnológica e adaptar a legislação penal às novas realidades. A pena básica para a conduta de invadir dispositivo informático é de detenção, de 3 (três) meses a 1 (um) ano, e multa. No entanto, a legislação prevê diversas agravantes que podem elevar significativamente a reprimenda penal, como a obtenção de dados sensíveis, a divulgação das informações obtidas e a invasão de dispositivos de autoridades públicas. (Texeira, 2024).

É importante destacar que as penas previstas para o crime em análise podem variar de acordo com as circunstâncias concretas do caso, sendo possível a aplicação de penas mais severas em situações que envolvam prejuízos econômicos significativos ou a violação de dados de grande relevância.

No entanto, com o propósito de tutelar crimes informáticos puros, esta legislação é ineficaz em vários pontos, principalmente por não antever a forma de violência moral nas condutas praticadas pelos cibercrimes. Nota-se que, como o caso da famosa Carolina Dieckmann teve grande repercussão na mídia, a sociedade acabou se movimentando para que

esta lei fosse aceita o quanto antes, sendo que era indispensável uma melhor elaboração pelos juristas e especialistas da referida área. Diante disso, observa-se que essa é uma das causas para que a referida lei tenha falhas, deixando, assim, a população vulnerável. (Ferreira, 2021).

Nota-se, por exemplo, uma grande insuficiência da Lei 12.737/2012, prevista no artigo 154-A do CP, que só considera crime se houver violação ao dispositivo de segurança. Assim, quando a vítima não dispõe de qualquer programa antivírus ou outro dispositivo que deixe seu dispositivo seguro, mesmo que seja violado virtualmente, não se enquadrará como invasão de dispositivo informático, pois é indispensável ter ultrapassado algum "mecanismo" de segurança. (Ferreira, 2021).

Também não se considera infração do artigo 154-A do Código Penal quando um colega de trabalho compartilha o computador com outro e descobre informações ou fotos dessa pessoa e as públicas. Nessa situação, mesmo que existisse o mecanismo de segurança no computador de trabalho, o agente não teve que ultrapassá-lo, descaracterizando a figura do crime. São inúmeras as formas que podem ocorrer invasões de dispositivos eletrônicos sem que a pessoa responsável seja penalizada, por pura deficiência do texto da lei. (Ferreira, 2021).

Por fim, os delitos de natureza cibernética exigem provas, principalmente de perícia, uma vez que é bastante difícil conseguir testemunhas para esse tipo de infração.

Após dois anos da criação da Lei 12.737/2012, surgiu a Lei do Marco Civil da Internet (Lei 12.965/2014), que mostra uma alteração conjunta nas áreas penal e civil, buscando uma proteção na área digital.

2.3.2 Lei 12.965/2014 (marco civil da internet)

O Marco Civil da Internet foi apresentado como um Projeto de Lei na Câmara dos Deputados em 2011, com o número PL 2.126/2011, e foi apensado ao PL 5.403/2001. Esse projeto resultou de sugestões da sociedade, coletadas por meio de uma consulta pública realizada pelo Ministério da Justiça. Sua sanção ocorreu no dia seguinte à aprovação no Senado Federal, durante a abertura do Encontro Multissetorial Global sobre o Futuro da Governança da Internet – NETmundial, que reuniu representantes de mais de 80 países em São Paulo. O evento gerou uma repercussão positiva em várias partes do mundo. Finalmente, em 23 de abril de 2014, a Lei nº 12.965 foi aprovada, estabelecendo princípios, garantias, direitos e deveres para o uso da Internet no Brasil (Brasil, 2014).

Conhecida como a Constituição da Internet Brasileira, essa lei tem como objetivo central estabelecer diretrizes para a regulamentação das relações entre as empresas que oferecem produtos e serviços vinculados à internet e os usuários que os utilizam em todo o território nacional (Brasil, 2014).

Ao abordar questões como privacidade, segurança, e direitos dos usuários, a lei busca criar um ambiente digital mais justo e transparente, promovendo a proteção dos dados pessoais e assegurando que as interações online sejam realizadas de forma responsável e ética. Dessa forma, a legislação visa não apenas regulamentar o setor, mas também fomentar a confiança dos cidadãos na utilização da internet como um espaço seguro e acessível.

O texto do Marco Civil da Internet estabelece princípios importantes, como a liberdade de expressão, pluralidade, diversidade, abertura, colaboração, exercício da cidadania, proteção da privacidade, dados pessoais, livre iniciativa, concorrência e defesa do consumidor. No entanto, ele não aborda diretamente temas que são regulamentados por outras leis, como cibercrimes, comércio eletrônico, direito autoral, expansão da banda larga e regulamentação das telecomunicações.

A lei foi criada para preencher lacunas no sistema jurídico em relação a crimes virtuais, começando por listar os direitos dos usuários. Ela trata de questões como o acesso aos dados de navegação e a atuação do poder público em casos de crimes online. O objetivo é garantir que os cidadãos possam usar a internet de forma autônoma e segura, sem sofrer prejuízos, sempre com a proteção de seus direitos.

A Lei nº 12.965/14, conhecida como Marco Civil da Internet, confirma as garantias constitucionais, mas não tipifica condutas criminosas. Sua proposta é ser a "Constituição da Internet Brasileira", abrangendo uma variedade de pontos importantes sobre direitos e garantias dos usuários. Como descreve Cassanti (2014, p. 91-92):

> Remoção de conteúdo: Conforme estipulado pelo Marco Civil da Internet, os provedores de conexão à internet não serão responsabilizados civilmente por danos decorrentes de conteúdo gerado por terceiros. Estas entidades não serão sujeitas a processos judiciais devido ao conteúdo publicado por seus usuários, exceto se, após ordem judicial, deixarem de adotar as medidas necessárias para tornar esse conteúdo indisponível dados pessoais: O Marco Civil garante aos usuários da internet o direito ao sigilo de suas comunicações online, exceto mediante ordem judicial. Além disso, estabelece a obrigação de fornecer informações claras e completas nos contratos de prestação de serviços, e proíbe o compartilhamento dos registros desses usuários com terceiros. Neutralidade da rede: Este princípio defende que os provedores responsáveis pela transmissão de dados devem tratar todos os pacotes de dados de forma igualitária, sem fazer distinção com base no conteúdo, origem ou destino. Este conceito é conhecido como neutralidade da rede.

Conforme o Marco Civil da Internet, os provedores são obrigados a guardar os registros por um período de um ano. Além disso, a lei autoriza que autoridades policiais ou

administrativas e o Ministério Público solicitem a preservação dos registros por mais alguns tempos, se necessário. O prazo padrão para retenção desses registros em provedores de registros é de seis meses, conforme estabelecido nos artigos 13 e 15.

> A legislação que regula o uso da internet no Brasil estabelece princípios essenciais, como a garantia da liberdade de expressão e comunicação, a proteção da privacidade e dos dados pessoais, a preservação da neutralidade de rede, a segurança e estabilidade da rede, a responsabilização dos agentes conforme suas atividades, a promoção da participação na rede e a liberdade dos modelos de negócios, desde que em consonância com os demais princípios estabelecidos (Brasil, 2019).

Os princípios que regem o uso da internet no Brasil estão descritos no Artigo 3º da lei:

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
>
> I - Garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
>
> II - Proteção da privacidade;
>
> III - Proteção dos dados pessoais, na forma da lei;
>
> IV - Preservação e garantia da neutralidade de rede;
>
> V - Preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
>
> VI - Responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
>
> VII - Preservação da natureza participativa da rede;
>
> VIII - Liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.
>
> Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte. (Brasil, 2019).

Os princípios elencados acima mostram como deve ser regida a internet e seu uso por todos os agentes, de forma que possa contribuir para o desenvolvimento da rede em seu aspecto físico quanto no social, além desenvolvimento intelectual no uso desta.

O Marco Civil da Internet apresenta algumas limitações, apesar de sua intenção de proteger os direitos dos usuários. A tentativa de aplicar ferramentas judiciais do mundo físico, como a necessidade de uma ordem judicial, no ambiente virtual pode ser contraproducente. Isso ocorre porque os ritmos dos dois mundos são muito diferentes: enquanto o mundo físico é mais lento, o mundo virtual demanda rapidez. Portanto, é urgente a necessidade de uma atualização legal que aborde de forma mais eficaz os crimes cibernéticos.

2.4 RESULTADOS E DISCUSSÃO

Neste estudo, foi realizada uma análise detalhada da legislação brasileira referente aos crimes virtuais, com foco nas Leis 12.737/12 (Lei Carolina Dieckmann) e 12.965/14 (Marco Civil da Internet). A seguir, são apresentados os principais resultados e discussões acerca da efetividade dessas leis no combate aos crimes cibernéticos, bem como das lacunas que ainda existem no ordenamento jurídico brasileiro para tratar adequadamente dessa questão emergente.

2.4.1 Limitações da Lei 12.737/12 no Combate aos Crimes Virtuais

A Lei 12.737/12, conhecida como Lei Carolina Dieckmann, representa um marco inicial para a regulamentação de crimes cibernéticos no Brasil, tratando especificamente da invasão de dispositivos informáticos. Contudo, apesar de seu caráter pioneiro, a aplicação da lei enfrenta desafios práticos significativos. Um dos principais entraves é a exigência de que o crime de invasão seja realizado mediante a violação de mecanismos de segurança do dispositivo. Isso implica que, em casos onde o dispositivo invadido não possua tais mecanismos, a conduta não é enquadrada como criminosa pela legislação atual, deixando diversas vítimas desprotegidas. Esse resultado aponta para a necessidade urgente de reformulação da lei, para que crimes de invasão sejam punidos independentemente da presença de mecanismos de segurança específicos no dispositivo.

Outro aspecto problemático é a exclusão de situações nas quais a invasão ocorre por meio de acesso físico, sem violação de software de segurança. Tal limitação restringe a aplicação da lei a apenas certos tipos de invasão, o que é insuficiente para um cenário de crimes virtuais que se desenvolvem e adaptam rapidamente. Assim, conclui-se que a Lei 12.737/12, embora tenha sido um avanço importante, precisa de atualizações que considerem a diversidade de métodos utilizados por criminosos cibernéticos e as mudanças tecnológicas que ocorrem continuamente.

2.4.2 Limitações do Marco Civil da Internet (Lei 12.965/14) em Relação à Proteção do Usuário

O Marco Civil da Internet, embora reconhecido como a "Constituição da Internet" brasileira, aborda temas como liberdade de expressão, proteção de dados e neutralidade de rede, mas não define diretamente tipos penais para crimes cibernéticos. Isso faz com que sua eficácia na prevenção de delitos virtuais seja limitada, pois a legislação não prevê punições

específicas para várias condutas ilícitas na internet, como golpes financeiros e extorsões que envolvem dados privados. Outro ponto observado é a complexidade burocrática para remoção de conteúdo prejudicial, exigindo ordem judicial para que os provedores sejam obrigados a agir. Em crimes virtuais, onde a rapidez é fundamental, a demora para obtenção de ordens judiciais pode impedir a proteção efetiva das vítimas. A legislação deveria permitir uma atuação mais ágil das plataformas e das autoridades para remover conteúdos potencialmente nocivos.

Comparando com legislações internacionais, como o Cybersecurity Information Sharing Act (CISA) dos Estados Unidos, observa-se que o Brasil está atrasado em termos de um sistema integrado que permita a troca de informações entre autoridades e provedores para a rápida identificação e contenção de crimes. Essa comparação destaca a necessidade de modernizar o Marco Civil para que ele inclua diretrizes de cooperação mais direta entre as empresas de tecnologia e as autoridades brasileiras.

A análise das limitações das Leis 12.737/12 e 12.965/14 revela que o Brasil precisa de reformas legislativas para lidar adequadamente com a criminalidade digital. Propõe-se que as seguintes áreas sejam consideradas para futuras atualizações legislativas:

Atualização da Lei 12.737/12: Remover a exigência de mecanismos de segurança específicos para caracterizar a invasão de dispositivo informático como crime. Essa mudança garantiria maior proteção para usuários que, mesmo dispondo de antivírus, têm seus dispositivos invadidos.

Inclusão de Novas Tipificações no Marco Civil da Internet: Para enfrentar a velocidade dos crimes cibernéticos, o Marco Civil poderia estabelecer penalidades específicas para condutas que causam danos diretos aos usuários, como roubo de dados e fraudes financeiras.

Agilidade na Remoção de Conteúdo Prejudicial: A legislação poderia adotar um sistema que permita a remoção de conteúdo nocivo de forma mais rápida, incluindo uma atuação mais efetiva dos provedores sem a necessidade de ordem judicial em situações de urgência.

Pode-se utilizar como exemplo a flexibilização da Lei 12.965/14 durante o período eleitoral. Devido aos curtíssimos prazos para apresentação de defesa, motivados pelo período ínfimo de campanha eleitoral, o TSE acabou por alterar a responsabilização dos provedores através da Resolução nº 23.732/24, impondo a responsabilidade sobre estes de remover o conteúdo sem a necessidade de decisão judicial. Embora polêmica e não seja o foco deste trabalho, foi a solução que o tribunal vislumbrou para minimizar possíveis prejuízos

enfrentados por candidatos e partidos eleitorais durante o processo de 2024, em decorrência de publicações realizadas na rede mundial de computadores (Leal, Lenh e Sirotheau, 2024).

Os resultados sugerem que a legislação brasileira ainda se mostra insuficiente para atender à demanda crescente de proteção contra crimes virtuais. A análise das lacunas legais destaca o desafio de manter uma legislação atualizada em um ambiente digital que se transforma constantemente. Sem atualizações que acompanhem esses avanços, a legislação permanece ineficaz, o que prejudica a confiança dos cidadãos na segurança digital e dificulta o combate eficiente aos crimes virtuais. Comparando os resultados com estudos realizados em países que estão à frente no combate a crimes virtuais, observa-se que a ausência de um arcabouço legal robusto deixa o Brasil vulnerável a ações de criminosos que encontram facilidade em explorar brechas nas leis. Este estudo reforça, portanto, a necessidade de aprimorar o ordenamento jurídico, criando mecanismos mais ágeis e eficazes para o combate aos crimes cibernéticos e ampliando a proteção aos direitos dos usuários no ambiente digital.

3 CONSIDERAÇÕES FINAIS

Este trabalho teve como objetivo explicar as limitações das leis brasileiras relacionadas aos crimes virtuais, com foco nas Leis 12.737/12 (Lei Carolina Dieckmann) e 12.965/14 (Marco Civil da Internet). A pesquisa demonstrou que, embora essas leis representem avanços iniciais, ainda apresentam limitações significativas na proteção eficaz dos cidadãos. A Lei 12.737/12 enfrenta desafios em sua aplicabilidade, pois exige a violação de mecanismos de segurança para caracterizar a invasão de dispositivos, deixando desprotegidos os usuários que não possuem tais proteções. O Marco Civil da Internet, embora estabeleça princípios importantes, não aborda diretamente questões relacionadas à segurança e à penalização de crimes virtuais.

A análise indica que é urgente uma atualização legislativa para acompanhar a evolução tecnológica e os métodos de crimes cibernéticos. Algumas sugestões incluem a ampliação da Lei 12.737/12 para proteger dispositivos que não possuam segurança específica e a inclusão de penalidades no Marco Civil da Internet para fraudes e roubo de dados. A pesquisa também destaca a importância de uma maior colaboração entre autoridades, provedores e a sociedade, além da adoção de diretrizes inspiradas em legislações internacionais que possam ser adaptadas ao contexto brasileiro.

Para garantir maior segurança no ambiente digital, é necessário um arcabouço jurídico mais robusto, que fortaleça a confiança dos usuários e previna, de forma eficaz, os crimes virtuais.

REFERÊNCIAS

AMARAL, L. D.; FERREIRA, J. M. Proteção de dados e segurança na era digital: análise do GDPR europeu e lições para o Brasil. *SciELO*, 2023.

BRASIL**. Código Penal, Decreto-Lei nº 2.848, de 7 de dezembro de 1940**. Atualizado pela Lei nº 13.964, de 24 de dezembro de 2019. Diário Oficial da União: Brasília, DF, 30 dez. 2019. Disponível em: https://www.jusbrasil.com.br/topicos/10618981/artigo-158-do-decreto-lei-n-2848-de-07-de-dezembro-de-1940. Acesso em: 30 out. 2024.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil de 1988.** Brasília, DF. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 30 out. 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. Brasília, DF: Palácio do Planalto, 2012 Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 24 set. 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. Diário Oficial da União: Brasília, DF, 23 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l12965.htm. Acesso em: 14 nov. 2024.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014. Diário Oficial da União: Brasília, DF, 15 ago. 2018. Seção 1, p. 1. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2018/lei/l13709.htm. Acesso em: 30 out. 2024.

BRASIL. **Lei nº 9.609, de 19 de fevereiro de 1998**. Dispõe sobre a proteção da propriedade intelectual e a regulamentação de programas de computador. Diário Oficial da União: Brasília, DF, 20 fev. 1998. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9609.htm. Acesso em: 30 out. 2024.

BRITO, Auriney. **Direito Penal Informático.** Rio de Janeiro: Saraiva Jur, 2013. E-book. pág.1. ISBN 9788502209428. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788502209428/. Acesso em: 15 nov. 2024.

CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas Reais.** 1. ed. Rio de Janeiro: Brasport, 2014.

CROZE, Hervé; BISMUTH, Yves. **Direito digital e processo eletrônico**. 8. ed. São Paulo: Saraiva, 2024.

DA SILVA, Patrícia Santos; SILVA, Matheus Passos. **Direito e crime cibernético: análise da competência em razão do lugar no julgamento de ações penais.** Editora Vestnik, 2015. Disponível em: https://profmatheus.com/wp-content/uploads/2017/05/direito-crime-cibernetico.pdf. Acesso em: 24 out. 2024.

FERREIRA, Sarah Pereira. **Crimes cibernéticos: a ineficácia da legislação brasileira**. 2021. Disponível em: https://repositorio.pucgoias.edu.br/jspui/handle/123456789/1709. Acesso em: 19 set. 2024.

GORGULHO, R. **Cybersecurity and Legislative Gaps in Brazil: A Comparative Analysis with International Norms**. *SSRN - Social Science Research Network*, 2024. Disponível em: http://www.ssrn.com/abstract_id=1234567. Acesso em: 24 set. 2024.

LEAL, Martha; LEHN, Izabela; SIROTHEAU, Débora. **A responsabilidade das plataformas digitais no cenário eleitoral.** Disponível em: https://www.inpd.com.br/post/a-responsabilidade-das-plataformas-digitais-no-cen%C3%A1rio-eleitoral. Acesso em: 14 nov. 2024.

PEREIRA, S. L.; OLIVEIRA, M. T. **A Inadequação da Lei Carolina Dieckmann no Combate aos Crimes Digitais no Brasil.** *Portal de Periódicos da CAPES*, 2022.
PINHEIRO, Patrícia P. **Direito Digital - 7ª Edição 2021**. 7ª edição. Rio de Janeiro: Saraiva Jur, 2021. E-book. pág.4. ISBN 9786555598438. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786555598438/. Acesso em: 15 nov. 2024.

PRADO, Luís Regis. **Direito Penal: parte geral. *3. ed. rev. e atual***. São Paulo: Editora Atlas, 2015.

SILVA, T. R.; SANTOS, C. R. **O Marco Civil da Internet e a Proteção de Dados: Limites e Potenciais para Segurança Digital.** *ResearchGate*, 2023.

TEIXEIRA, Tarcísio. **Direito Digital e Processo Eletrônico - 8ª Edição 2024**. 8ª edição. Rio de Janeiro: Saraiva Jur, 2024. *E-book.* pI ISBN 9788553622344. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788553622344/. Acesso em: 15 nov. 2024.

VAZ, N. A.; MENDES, F. C. **Crimes Cibernéticos e o Ordenamento Jurídico Brasileiro: Desafios e Perspectivas**. Revista Brasileira de Direito Penal e Criminologia, *2023*.