FAHESP - FACULDADE DE CIÊNCIAS HUMANAS, EXATAS E DA SAÚDE DO PIAUÍ
AFYA FACULDADE PARNAÍBA
CURSO DE DIREITO
DISCIPLINA DE TRABALHO DE CONCLUSÃO DE CURSO II

OS DESAFIOS DA LEGISLAÇÃO BRASILEIRA NO COMBATE AOS CRIMES CIBERNÉTICOS: IDENTIFICAÇÃO DAS LACUNAS E PROPOSTAS DE APRIMORAMENTO

ADRIELE DA SILVA SANTOS

ANA BEATRIZ PRADO CAMPOS

AMANDHA DOS SANTOS ARAÚJO

PARNAÍBA/PI

2025

ADRIELE DA SILVA SANTOS
ANA BEATRIZ PRADO CAMPOS
AMANDHA DOS SANTOS ARAÚJO

OS DESAFIOS DA LEGISLAÇÃO BRASILEIRA NO COMBATE AOS CRIMES CIBERNÉTICOS: IDENTIFICAÇÃO DAS LACUNAS E PROPOSTAS DE APRIMORAMENTO

Projeto de pesquisa apresentado à disciplina de Trabalho de Conclusão de Curso II como requisito para obtenção de nota no Curso FAHESP/AFYA PARNAÍBA.

Direito Professor da Disciplina: GEILSON SILVA PEREIRA.

PARNAÍBA/PI

2025

RESUMO:

O presente trabalho de conclusão de curso tem como objetivo analisar os desafios da legislação brasileira no combate aos crimes cibernéticos, destacando a necessidade de atualização normativa diante da complexidade das condutas digitais. O estudo parte do conceito de crime sob diferentes perspectivas doutrinárias, aborda a evolução da internet e como o meio digital se tornou um espaço tanto de benefícios quanto de riscos, possibilitando a prática de delitos no campo virtual. No plano internacional, destaca-se a Convenção de Budapeste (2001) como marco de cooperação e harmonização legislativa, ainda que o Brasil não seja signatário formal. No cenário nacional, são ressaltados avanços normativos como a Lei Carolina Dieckmann (n° 12.737/2012), o Marco Civil da Internet (n° 12.965/2014), a LGPD (n°13.709/2014) e a Lei nº 14.155/2021, que agrava penas para crimes eletrônicos. Apesar dos avanços, persistem lacunas na legislação e na aplicação prática, dificultando a persecução penal e a proteção efetiva de direitos fundamentais. A pesquisa adota metodologia bibliográfica e documental, com enfoque qualitativo, buscando contribuir para o debate acadêmico e para a proposição de soluções jurídicas que fortaleçam o enfrentamento aos delitos cibernéticos no Brasil.

Palavras-chave: Crimes Cibernéticos. Lei Carolina Dieckmann. Marco Civil da Internet.

1 INTRODUÇÃO

O presente artigo tem como propósito examinar os desafios da legislação brasileira no combate aos crimes cibernéticos, buscando compreender suas implicações jurídicas e sociais dentro do contexto nacional. Parte-se da premissa de que a norma ainda não acompanha de forma eficaz a complexidade dos crimes praticados no ambiente digital, como por exemplo o estelionato virtual e as suas atualizações na possibilidade de cometimento, o que torna imprescindível refletir sobre os fatores que influenciam e moldam o desenvolvimento dessa temática.

Sob esse viés, é importante destacar o conceito de crime. Conforme Greco (2025, p. 159-160), conceitua crime sob três perspectivas, sendo a primeira concepção a formal que consiste sendo “crime é toda conduta que atente, que colida frontalmente contra a lei penal editada pelo Estado”. A segunda abordagem é a material, que corresponde “crime é toda que viole (ou ameace) os bens jurídicos mais importantes e necessários ao convívio e sociedade”. Por fim, a terceira visão constitui ao analítico que equivale a “crime é toda conduta típica, antijurídica e culpável (conceito tripartido do crime)”.

Outrossim, é indispensável para a pesquisa compreender o significado da internet, segundo Biolcati (2022, p.27-28): “a internet conceitua-se como uma rede mundial de computadores interligados entre si, que compartilham, para esse fim, um conjunto de protocolos denominado TCP/IP, a permitir a troca de dados entre aqueles”. Nesse ínterim, a partir da introdução da internet no cotidiano das pessoas e das empresas trouxe consigo inúmeras vantagens, como a possibilidade de realizar compras on-line, videochamadas, efetuar transações financeiras, ou seja, tudo com a finalidade de facilitar atividades estando apenas navegando virtualmente.

Portanto, o presente trabalho busca analisar como a ferramenta da internet tornou-se um instrumento para os criminosos cometerem delitos virtuais e ainda a sua disseminação e aprimoramento. Consoante a isso, o crescimento alarmante dessas práticas gera tanto danos psicológicos como financeiros às vítimas, e representaram um grande desafio para as autoridades, que enfrentam dificuldades na punição dos responsáveis devido ao grande avanço tecnológico explorado por criminosos.

Conforme isso, é possível notar que o cometimento de crimes cibernéticos tem um impacto negativo que influencia a economia nacional, tendo em vista, que todas as pessoas podem ser vítimas desses criminosos e ter seu patrimônio econômico abalado. Portanto, com as crescentes modalidades de delitos virtuais é necessário que o Estado esteja preparado para proteger toda a população que venha a sofrer com esses ataques.

Logo, o objetivo do trabalho pauta-se na necessidade de estudar quais são os desafios enfrentados pelo legislador brasileiro na tipificação e combate aos atuais crimes cibernéticos, pois constituem um problema emergente. Nessa vereda, serão analisadas as legislações vigentes acerca do assunto, como a Lei Geral de Proteção de Dados (LGPD), Lei Carolina Dieckmann (Lei nº 12.737/2012), entre outras. Ademais, será pesquisado como o crime de estelionato teve sua adaptação aos meios digitais, implicações jurídicas e ainda como é possível tecer uma analogia ao combate desse delito no estado do Piauí.

A pesquisa será fundamentada em revisão bibliográfica e documental, adotando uma abordagem teórica e reflexiva, de caráter qualitativo, com vistas a permitir uma análise crítica dos conceitos, normas e interpretações relacionadas à temática. Para alcançar tais propósitos, o trabalho será estruturado em eixos temáticos que permitirão abordar desde os fundamentos teóricos até as implicações práticas e os possíveis desdobramentos jurídicos ou institucionais.

Essa pesquisa representa a etapa final para a elaboração do artigo científico desenvolvido na disciplina de Trabalho de Conclusão de Curso II (TCC2). Depois consolidar as bases teóricas, os recortes metodológicos e a definição clara do problema de pesquisa, espera-se que o trabalho aqui delineado sirva como guia sólido para uma investigação aprofundada, crítica e socialmente relevante, que contribuirá para o debate acadêmico e para a construção de soluções fundamentadas no campo de Direito digital.

2. DESENVOLVIMENTO

2.1 Conceitos e Evolução dos Crimes Cibernéticos no Contexto Jurídico

Os crimes cibernéticos, também denominados delitos informáticos, consistem em condutas ilícitas praticadas por meio da tecnologia da informação e comunicação, por meio de sistemas computacionais ou dispositivos digitais como

meio ou fim da infração. A doutrina majoritária os define como toda conduta típica, ilícita e culpável que tenha por objeto ou instrumento o ambiente digital. Esses crimes podem variar desde invasão de sistemas e roubo de dados até ataques mais complexos que visam a infraestrutura crítica, o que vem se aperfeiçoando constantemente.

Os delitos, mesmo no ambiente virtual, surgem como resposta ao uso desvirtuado da liberdade humana. Rogério Greco (2025, vol.1 -27ª, p.13) destaca que “o homem não nasceu para ficar preso. A liberdade é uma característica fundamental do ser humano. A história da civilização demonstra, no entanto, que, logo no início da criação, o homem se tornou perigoso para seus semelhantes”.

Essa reflexão demonstra que a liberdade seja um direito inerente, contudo sua má utilização exige mecanismos de contenção, dentre eles o Direito Penal, que se reinventa de forma gradativa para acompanhar as novas formas de lesão aos bens jurídicos, contudo é possível, ainda, analisar a grande dificuldade das leis e jurisprudências de acompanharem o avanço da criminalidade virtual.

Atualmente, a doutrina e a jurisprudência reconhecem que os crimes cibernéticos desafiam princípios do Direito Penal, como a tipicidade, territorialidade e legalidade, em razão da velocidade com que surgem novas condutas. Doutrinadores como Guilherme de Souza Nucci defendem a aplicação extensiva e a interpretação analógica quando houver lacunas, enquanto outros, como Luiz Flávio Gomes, apontavam a necessidade de contínua atualização legislativa para assegurar a segurança jurídica e evitar a violação do princípio da legalidade.

Reforça-se assim, a ideia de que a evolução legislativa não visa restringir a liberdade individual, mas sim equilibrá-la com a necessidade de proteger direitos fundamentais em um ambiente virtual que potencializa riscos. A evolução legislativa brasileira no combate aos crimes cibernéticos acompanha a crescente relações sociais e econômicas, como é ausência de Tipificação Específica, Marco Inicial de Regulação (Lei nº 12.737/2012), Consolidação Normativa (Lei nº 12.965/2014), Aprofundamento (Lei nº 13.709/2018 e Tipificações Recentes e Atualizações (Lei nº 14.155/2021).

Por outro lado, observa-se que o conceito de internet, nada mais é que a conexão de diversas redes de computadores que se conectam com os demais para compartilhar informações. Com isso, a criação da internet trouxe vantagens significativas, como a interligação de pessoas em diferentes lugares do mundo,

facilitando a comunicação e as transações financeiras. Mas, em contrapartida obteve um aumento significativo da possibilidade de cometimento de novos delitos.

Segundo a Convenção de Budapeste elaborada na Hungria em 23 de novembro de 2001, um dos principais e principais tratados internacionais voltados exclusivamente para o combate sobre o tema, elaborada pelo Conselho da Europa, contou com a participação de diversos países, inclusive não europeus, cujo objetivo central seria a necessidade de buscar prioritariamente uma política criminal comum destinada à proteção da sociedade contra o crime cibernético, como harmonizar a legislação, aperfeiçoar as técnicas investigativas e fomentar a cooperação internacional.

A partir desta Convenção os crimes puderam ser classificados os crimes cibernéticos puros são aqueles que só podem ser cometidos no meio digital, que são as invasões de sistemas, tendo como objetivo exclusivo o sistema de computador. Paralelamente, crimes cibernéticos mistos são crimes que vão se adaptando para o meio digital, como estelionato eletrônico e até exploração sexual infantil na internet.

O Brasil não é signatário formal da Convenção de Budapeste, mas tem utilizado suas diretrizes como referência na formulação de políticas públicas e legislação nacional, especialmente após a Lei 12.737/2012 (Lei Carolina Dieckmann) e o Marco Civil da Internet (Lei 12.965/2014), trazendo assim uma grande importância para o contexto jurídico atual. A Convenção representa uma resposta internacional pioneira aos desafios desses delitos, que, pela sua natureza difusa, exigem a superação de barreiras tradicionais, como territorialidade e soberania absoluta.

Conforme Leite e Lemos (2014), o Marco Civil da Internet traz um importante rol de princípios capazes de proteger usuários, empreendedores e a própria característica de abertura da internet, que é indubitavelmente um importante marco na implementação da Internet no Brasil, escrito por George Salomão Leite e Ronaldo Lemos.

O avanço da tecnologia e popularização da internet intensificou a ocorrência de crimes virtuais, trazendo consigo desafios inéditos para o Direito como um todo, como a falta de regulamentação para novas modalidades de crimes digitais e dificuldade na obtenção de provas eletrônicas. Esses crimes geram impactos econômicos, como perdas financeiras e custos de segurança.

No Brasil, a evolução da legislação voltada para os crimes digitais ocorre de forma gradual com o impulsionamento de casos de grande repercussão, entretanto é indispensável mencionar que esses avanços foram de suma importância, mas ainda há desafios significativos a serem superados. A legislação precisa estar sendo atualizada constantemente para enfrentar esses desafios, ademais normas eficazes são essenciais para proteger a sociedade dos perigos do meio digital.

O combate aos crimes cibernéticos está em constante evolução, exigindo inovação tecnológica, novas estratégias de proteção e adaptação das legislações para acompanhar o avanço das ameaças digitais. Além disso, a análise das lacunas permite uma melhor compreensão dos impactos, tanto sociais como jurídicos, dos crimes cibernéticos, que por sua vez é uma realidade complexa, fortalecendo o papel da justiça na proteção dos direitos fundamentais nos ambientes digitais.

Vale ressaltar que a proteção de dados, consiste em um direito e garantia fundamental elencada em seu Artigo 5º, LXXIX, da Constituição Federal:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais

Logo é de suma importância garantir aos usuários da internet maior segurança e respaldo jurídico. As matérias em que tratam do referido tema podem ser encontradas em diferentes leis, Código Penal, Constituição Federal, entre outros.

2.2 A Regulamentação dos Crimes Cibernéticos após a Lei de Proteção de Dados e a Lei Carolina Dieckmann

É indubitável compreender o conceito dos cibercrimes, que consiste a partir de Pinheiro (2010, p. 46-47) sendo:

> Os crimes digitais podem ser conceituados como sendo as condutas de acesso não autorizado a sistemas informáticos, ações destrutivas nesses sistemas a interceptação de comunicações, modificações de dados, infrações a direitos de autor, incitação ao ódio e descriminação, escárnio religioso, difusão de pornografia infantil, terrorismo entre outro.

Logo, é necessário entender como os legisladores tratam essa matéria com a finalidade de proteger os cidadãos. Nota-se que a implementação da internet no cotidiano da população, trouxe inúmeras vantagens, bem como ocasionou aumentos significativos aos desafios relacionados à segurança pública que impactam diretamente a segurança digital dos cidadãos, a proteção de dados e a estabilidade das instituições.

Um marco importante é a Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, que alterou o Código Penal para tipificar condutas como a invasão de dispositivos eletrônicos, dando um avanço inicial no combate aos crimes cibernéticos no Brasil. Através desse incidente, a atriz teve seu computador invadido por meio do e-mail, onde os hackers conseguiram ter acesso a fotos íntimas e ainda tentaram extorqui-la.

A consequência jurídica dessa lei foi a inserção de dois dispositivos no Código Penal, Art. 154-A e 154-B, intitulado como "Invasão de dispositivo informático". Dispõem o Art. 154-A, do Código Penal:

> Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita:
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.

Portanto, a conduta de invadir dispositivos eletrônicos sem a autorização pessoal passou a ser crime. Contudo, com o crescimento e expansão da internet, esses criminosos passaram a se adaptar com as circunstâncias presentes. Com o fito de proteger os dados pessoais e as relações entre usuário e internet, foi instituído no ordenamento o Marco Civil da Internet - Lei nº 12.965/2014 - que trouxe as primeiras considerações, princípios, conceitos, direitos e deveres acerca do tema.

Conforme Gonçalves (2016, p.210-211) evidencia que "O Marco Civil deveria ser um guia de orientação para todas essas questões e outras mais, que são construídas diuturnamente com o uso das tecnologias de informação e comunicação". Por conseguinte, o artigo 1º da referida lei, ressalta ainda que:

> Art. 1º Esta Lei estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria.

Dessa maneira, após a criação da lei da Carolina Dieckmann em que introduziu dois dispositivos no Código Penal, o marco civil da internet trouxe as

primeiras considerações do tema de extrema relevância, configurando o poder estatal o papel de proteger a relação da população com a utilização da internet. Ademais, apresentou conceitos de valor significativo para o estudo do assunto, estabelece o Artigo 5º da referida lei:

> Art. 5º Para os efeitos desta Lei, considera-se:
> I - internet: o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes;
> II - terminal: o computador ou qualquer dispositivo que se conecte à internet.

Outra importante legislação que trata do tema é a Lei Geral de Proteção de Dados Pessoais- Lei nº 13.709/18- que tem como objetivo complementar o Marco Civil da Internet. Conforme Filho (2021, p.100-101), dispõe que:

> A LGPD complementa a Lei no. 12.965/2014 – Marco Civil da Internet, cujo art. 3º,III, prevê como um dos princípios do uso da Rede, “a proteção dos dados pessoais, na forma da lei”. Entretanto, a LGPD vai além da Internet: de acordo com seu art. 3º, a lei se aplica a qualquer operação de tratamento realizada por pessoa natural ou jurídica, de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados”.

Ademais, instituiu em seu Artigo 1º, o seguinte:

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Conclui-se que o legislador ao inserir a LGPD no ordenamento jurídico, partiu da finalidade de proteger os dados pessoais da população. Por conseguinte, estabeleceu fundamentos, destinação, conceitos, princípios dentre outras considerações importantes. Observa-se ainda que a proteção desses dados passou a ser um direito e garantia fundamental ao cidadão, elencado no Artigo 5º, inciso LXXIX, da Constituição Federal, incluído pela Emenda Constitucional nº 115 de 2022.

Outrossim, cabe ressaltar a migração de alguns dispositivos penais para o meio virtual, como é o caso do estelionato. Que consiste em uma possibilidade de uma fraude eletrônica que tem sido muito utilizada pelos criminosos, através disso a lei 14.155/2021 alterou o Código Penal para tipificar essas condutas, instituindo o §2º-A do Artigo 171, CP. Nesse sentido, verifica-se que o ordenamento jurídico

caminha junto às problemáticas enfrentadas na atualidade, objetivando a proteção dos direitos e garantias da população.

2.3 Crimes Cibernéticos no Contexto Regional: uma Análise Jurídico-Social em Parnaíba-PI

Em Parnaíba, o uso de redes sociais, aplicativos de mensagens e serviços digitais passaram a integrar de forma significativa a vida cotidiana da população. Essa realidade, se por um lado amplia as oportunidades de comunicação, negócios e acesso à informação, por outro lado aumenta a exposição a riscos relacionados a golpes virtuais, fraudes financeiras e invasões de contas. A ampliação do acesso à internet, a crescente utilização de dispositivos móveis e a popularização das redes sociais na região ampliam o campo de atuação dos agentes criminosos, tornando a sociedade local igualmente vulnerável.

Nesse sentido, a realidade parnaibana insere-se no contexto nacional de enfrentamento a ilícitos virtuais, exigindo atenção tanto do ponto de vista jurídico quanto social. Assim, o mesmo ambiente que promove inclusão digital e dinamiza a economia local também se torna um espaço suscetível a práticas ilícitas, exigindo maior atenção da sociedade e das instituições responsáveis pela segurança.

Observa-se que a expansão digital em Parnaíba tem promovido maior inclusão social, possibilitando o acesso a serviços públicos e privados de forma remota. Contudo, o mesmo processo que favorece a integração da população ao ambiente virtual gera um aumento nas práticas delituosas relacionadas ao uso da tecnologia. Entre as ocorrências mais comuns destacam-se golpes financeiros em aplicativos de mensagens e redes sociais, bem como fraudes relacionadas a transações bancárias e ao comércio eletrônico, fenômenos que acompanham a dinâmica da sociedade brasileira como um todo. Nesse ínterim, é possível observar que os criminosos que se utilizam do meio cibernético para o cometimento de delito se aperfeiçoam cada vez mais.

Criminosos digitais frequentemente obtêm acesso a senhas de redes sociais e, fingindo ser a vítima, aplicam golpes em seus contatos. Consequentemente aplicando golpes e quando estes vão descobrir, pode ser tarde, esse é o famoso “Golpe do Pix", onde os criminosos que praticam esse delito, se especializam cada vez mais. Os golpes envolvendo Pix e WhatsApp são alguns dos crimes cibernéticos

mais comuns atualmente no Brasil. Eles combinam engenharia social, manipulação emocional e vulnerabilidades tecnológicas para enganar as vítimas. Com isso, os cibercrimes estão cada vez mais sofisticados, contudo, a melhor defesa é a informação. Manter-se atualizado, desconfiar de situações fora do comum e adotar medidas simples de segurança digital pode evitar prejuízos financeiros e emocionais.

Segundo dados do Banco Central do Brasil, apenas em 2023 foram registradas mais de 1,5 milhão de tentativas de fraude envolvendo o sistema Pix, evidenciando o crescimento exponencial deste tipo de cibercrime. Além disso, golpes combinando uso de WhatsApp clonado com solicitações de transferências financeiras são cada vez mais comuns. De acordo com levantamento do Laboratório de segurança digital da PSafe, somente no primeiro semestre de 2023 foram detectadas mais de 3,8 milhões de tentativas de golpes via WhatsApp no Brasil.

Do ponto de vista normativo, o ordenamento jurídico brasileiro dispõe de mecanismos para o enfrentamento dessas práticas, com destaque para a Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, e a Lei nº 12.965/2014, o Marco Civil da Internet. Ambas estabelecem parâmetros para responsabilização e proteção de dados, aplicando-se também à realidade de municípios como Parnaíba-PI. Todavia, a aplicação prática dessas normas encontra desafios consideráveis no âmbito regional, especialmente em razão de ainda haver necessidade de aperfeiçoamento de conhecimentos técnicos e estruturais enfrentados pelas autoridades locais.

A estrutura de segurança pública na cidade, embora desempenhe papel essencial no combate à criminalidade, onde há cursos especializados disponíveis para conhecimento de crimes cibernéticos, ainda carece de recursos técnicos especializados que permitam uma atuação mais eficaz frente aos delitos virtuais. Dessa forma, torna-se necessária uma maior articulação entre as instâncias regionais e as esferas estaduais e federais, de modo a fortalecer a atuação das autoridades competentes.

Do ponto de vista social, os crimes cibernéticos em Parnaíba-PI produzem impactos que vão além das perdas financeiras. As vítimas de golpes virtuais frequentemente enfrentam abalos emocionais e psicológicos, além de uma crescente desconfiança no uso das ferramentas digitais. Esse cenário compromete a credibilidade das interações virtuais e pode afetar o cotidiano da comunidade, uma

vez que limita a confiança necessária para a realização de transações comerciais, educacionais e sociais em ambiente online.

Nesse contexto, a educação digital surge como instrumento indispensável de prevenção. Em cidades em processo de adaptação à cultura tecnológica, como Parnaíba, a promoção de campanhas educativas voltadas para o uso seguro da internet contribui para a redução da vulnerabilidade dos usuários. A conscientização acerca de práticas de segurança, como a proteção de senhas, a verificação de informações e a desconfiança frente a contatos desconhecidos, constitui um mecanismo de proteção social que complementa a atuação repressiva do Estado.

Ademais, a realidade regional demonstra que os crimes cibernéticos em Parnaíba guardam estreita relação com a popularização das redes sociais, que se tornaram espaço privilegiado para a prática de fraudes e golpes. Esse fenômeno, embora presente em todo o país, adquire características particulares em razão do perfil sociocultural da população local. Assim, além da aplicação das normas nacionais, torna-se essencial a elaboração de estratégias adaptadas à realidade regional, que considerem as especificidades do município e sua dinâmica social.

No aspecto jurídico, a legislação brasileira oferece instrumentos claros para a prevenção e repressão dos crimes cibernéticos. A Lei nº 12.737/2012, por exemplo, tipifica a invasão de dispositivos informáticos e estabelece punições específicas para condutas que comprometem a segurança de dados. Já o Marco Civil da Internet, Lei nº 12.965/2014, estabelece princípios fundamentais, direitos e deveres para o uso da rede, garantindo proteção à privacidade, segurança e liberdade de expressão dos usuários. Além disso, o Código Penal, em artigos como o 155, crime de furto, artigo 171, crime de estelionato e artigo 266, crime de apologia de crime pode ser aplicado quando há elementos digitais que caracterizem fraude, apropriação indevida ou danos a terceiros:

> Art. 155 - Subtrair, para si ou para outrem, coisa alheia móvel;
> Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento;
> Art. 266 - Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento.

A articulação desses dispositivos legais demonstra que, embora a legislação seja nacional, sua aplicação em Parnaíba é essencial para orientar a atuação das autoridades locais, subsidiar investigações e promover a responsabilização dos

infratores. Além disso, a presença de normas claras e específicas contribui para a padronização dos procedimentos investigativos, fortalece a atuação preventiva e educativa junto à população e reforça a importância de medidas integradas entre órgãos de segurança pública, judiciário e instituições de ensino, visando reduzir a vulnerabilidade dos cidadãos frente às ameaças digitais.

Portanto, a análise jurídico-social dos crimes cibernéticos em Parnaíba evidencia que o enfrentamento desse fenômeno deve ser conduzido por uma abordagem integrada, que envolva não apenas a aplicação do ordenamento jurídico, mas também a capacitação das instituições locais e o engajamento da sociedade civil. A prevenção e a repressão eficazes demandam, de um lado, o fortalecimento das estruturas de segurança pública e, de outro, a conscientização da população sobre os riscos inerentes ao uso da internet. Assim, o combate aos crimes cibernéticos na região constitui desafio que exige esforços conjuntos do poder público e da coletividade.

3 CONSIDERAÇÕES FINAIS

O presente trabalho teve como finalidade analisar os desafios da legislação brasileira no combate aos crimes cibernéticos, enfatizando suas lacunas e refletindo sobre propostas de aprimoramento normativo e institucional. A pesquisa demonstrou que, apesar da existência de legislações relevantes voltadas para a proteção digital, ainda persistem limitações que dificultam a efetividade da aplicação do Direito diante das novas modalidades de delitos virtuais.

Constatou-se que leis como a Lei Carolina Dieckmann (Lei nº 12.737/2012), o Marco Civil da Internet (Lei nº 12.965/2014), a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e a Lei nº 14.155/2021 (Lei dos Crimes Cibernéticos) representaram avanços significativos no ordenamento jurídico brasileiro. Entretanto, a velocidade com que surgem novas formas de criminalidade digital supera a capacidade legislativa e institucional de resposta, o que fragiliza a proteção dos cidadãos.

Verificou-se, ainda, que a internet, ao mesmo tempo em que trouxe benefícios inegáveis para a sociedade, intensificou os riscos de invasão de dispositivos, fraudes eletrônicas e também violações à privacidade, com golpes atuais. Essas condutas refletem diretamente na vida cotidiana das pessoas e empresas,

impactando não apenas a esfera patrimonial, mas também a psicológica e social das vítimas.

No campo internacional, destacou-se a Convenção de Budapeste como referência fundamental para a cooperação e harmonização legislativa no combate aos crimes cibernéticos. Embora o Brasil não seja signatário formal, suas diretrizes têm influenciado a formulação de políticas públicas e de normas nacionais, revelando a importância da integração internacional no enfrentamento a delitos que não conhecem fronteiras territoriais.

No contexto regional, a análise realizada sobre a realidade de Parnaíba-PI demonstrou que os crimes cibernéticos repercutem de forma direta na vida da população local. Golpes como o do Pix e fraudes em redes sociais revelam a vulnerabilidade social diante da sofisticação crescente das práticas ilícitas. Assim, tornou-se evidente que a aplicação das normas nacionais encontra entraves estruturais e técnicos, o que reforça a necessidade de maior capacitação e integração das autoridades locais.

Outro ponto relevante evidenciado pela pesquisa foi a dimensão social dos crimes cibernéticos. Os danos não se limitam às perdas financeiras, mas incluem também abalos emocionais e a perda de confiança na utilização de ferramentas digitais. Esse cenário compromete a credibilidade das relações virtuais e pode afetar a economia e o desenvolvimento local, exigindo medidas de prevenção e conscientização contínuas.

Diante do exposto, reforça-se que o enfrentamento dos crimes cibernéticos deve ser conduzido por meio de uma abordagem multifacetada. É imprescindível combinar atualização legislativa, investimentos em infraestrutura tecnológica, fortalecimento das instituições e implementação de políticas públicas que promovam a proteção de dados, a segurança digital e a conscientização da sociedade.

Portanto, conclui-se que a presente pesquisa contribui para o debate acadêmico e jurídico ao evidenciar a necessidade de constante evolução do ordenamento jurídico brasileiro frente às demandas impostas pelo meio digital. Espera-se que tais reflexões estimulem novas discussões e a construção de soluções capazes de harmonizar os avanços tecnológicos com a proteção dos direitos fundamentais, assegurando um ambiente virtual mais seguro, inclusivo e confiável para toda a coletividade.

REFERÊNCIAS BIBLIOGRÁFICAS

BIOLCATI, Fernando Henrique De O. **Internet, Fake News e Responsabilidade Civil das Redes Sociais.** (Coleção Direito Civil Avançado). São Paulo: Grupo Almedina, 2022. E-book. p.27. ISBN 9786556276410. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786556276410/.Acesso em: 21 ago. 2025.

BRASIL. **Lei n.º 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*, Brasília, DF, 24 abr. 2014. Acesso em: 23 set. 2025.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Brasília, DF: Presidência da República, 5 out. 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 23 set. 2025.

BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018.** Dispõe sobre a proteção de dados pessoais. *Diário Oficial da União*, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 23 set. 2025.

BRASIL. **Lei nº 14.155, de 3 de maio de 2021.** Dispõe sobre crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet, entre outras providências. Presidência da República, 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14
155.htm. Acesso em: 20 out. 2025.

CASE, Steve. **A Terceira Onda da Internet.** Rio de Janeiro: Editora Alta Books, 2019. E-book. p.I. ISBN 9788550816869. Disponível em: https://app.minhabiblioteca.com.br/reader/books/9788550816869/. Acesso em: 23 set. 2025.

FILHO, Eduardo T. **A Lei Geral de Proteção de Dados Brasileira.** São Paulo: Grupo Almedina, 2021. E-book. p.103. ISBN 9786556271705. Disponível em: https://app.minhabiblioteca.com.br/reader/books/9786556271705/. Acesso em: 23 set. 2025.

GRECO, Rogério. **Curso de Direito Penal**. Vol.1 - 27ª Edição 2025. 27. ed. Rio de Janeiro: Atlas, 2025. E-book. p.158. ISBN 9786559776801. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786559776801/.Acesso em: 21 ago. 2025.

GONÇALVES, Victor Hugo P. **Marco Civil da Internet Comentado**. 1ª Edição 2017. Rio de Janeiro: Atlas, 2016. E-book. p.1. ISBN 9788597009514. Disponível em: https://app.minhabiblioteca.com.br/reader/books/978859700951 4/. Acesso em: 23 set. 2025.

LAKATOS, Eva M. **Fundamentos de Metodologia Científica.** 9. ed. Rio de Janeiro: Atlas, 2021. E-book. p.1. ISBN 9788597026580. Disponível em:

https://app.minhabiblioteca.com.br/reader/books/9788597026580/. Acesso em: 23 set. 2025.

MARCONI, Marina de A.; LAKATOS, Eva M. **Metodologia Científica**. 8. ed. Rio de Janeiro: Atlas, 2022. E-book. p.Capa. ISBN 9786559770670. Disponível em: https://app.minhabiblioteca.com.br/reader/books/9786559770670/. Acesso em: 23 set. 2025.

PINHEIRO, Patrícia Peck. **Direito digital global e seus princípios fundamentais**. Revista Jurídica, São Paulo, p. 46-47, 2016.

SARAIVA, Editora. **Lei geral de proteção de dados (LGPD) e marco civil da internet.** Rio de Janeiro: Expressa, 2022. E-book. p.7. ISBN 9786553620384. Disponível em: https://app.minhabiblioteca.com.br/reader/books/978655362038 4/. Acesso em: 23 set. 2025.