



PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA DE DIREITO E RELAÇÕES INTERNACIONAIS
NÚCLEO DE PRÁTICA JURÍDICA
COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO
ARTIGO CIENTÍFICO

OS CRIMES CIBERNÉTICO: DESAFIOS E IMPLICAÇÕES LEGAIS NA ERA DIGITAL

ORIENTANDA: MARIA EDUARDA RODRIGUES FLORES
ORIENTADOR (A): PROF. (A). MS. EDWIGES CONCEIÇÃO CARVALHO CORRÊA

GOIÂNIA
2025

MARIA EDUARDA RODRIGUES FLORES

OS CRIMES CIBERNÉTICO: DESAFIOS E IMPLICAÇÕES LEGAIS NA ERA DIGITAL

Projeto de Artigo Científico apresentado a Disciplina:
Trabalho de Curso I, da Escola de Direitos e Relações
Internacionais, Curso Bacharelado em Direito, da
Pontifícia Universidade Católica de Goiás (PUC-
GOIÁS). Prof. (a). Ms. Orientador (a): Edwiges
Conceição Carvalho Corrêa.

GOIÂNIA

2025

MARIA EDUARDA RODRIGUES FLORES

CRIMES CIBERNÉTICO: DESAFIOS E IMPLICAÇÕES LEGAIS NA ERA DIGITAL

Data da Defesa: ____/____/____

BANCA EXAMINADORA

Assinatura: _____

Nota: _____ Orientadora:

Assinatura: _____

Nota: _____ Examinador Convidado:

SUMÁRIO

RESUMO.....	05
INTRODUÇÃO.....	06
1. Secção I - HISTÓRICO DOS CRIMES CIBERNÉTICOS NO BRASIL.....	08
1.2 CONCEITO E A TIPOLOGIA DOS CRIMES CIBERNÉTICOS.....	10
1.3 As Características e as Modalidades de Crimes Digitais.....	12
2. Secção II - AS LACUNAS LEGISLATIVAS NO ORDENAMENTO JURÍDICO BRASILEIRO.....	13
2.2 AS DIFICULDADES NA RESPONSABILIZAÇÃO DOS INFRATORES.....	15
2.3 Os Desafios no Uso das Tecnologias da Vigilância Digital.....	17
3. Secção III -CASO CONCRETO (FRAUDE DIGITAL)	18
3.2 A RESPONSABILIDADE PENAL DOS AGENTES.....	21
3.3. As Propostas de Políticas Públicas para Combater os Golpes Cibernéticos.....	23
CONCLUSÃO.....	24
REFERÊNCIAS BIBLIOGRÁFICAS.....	27

OS CRIMES CIBERNÉTICO: DESAFIOS E IMPLICAÇÕES LEGAIS NA ERA DIGITAL

¹ Maria Eduarda Rodrigues Flores

O estudo analisou os crimes cibernéticos como fenômeno jurídico emergente decorrente da expansão tecnológica e da crescente utilização da internet nas relações sociais e comerciais. O objetivo consistiu em compreender os principais desafios enfrentados pelo ordenamento jurídico brasileiro na repressão e prevenção dessas práticas ilícitas. Adotou-se como método a pesquisa bibliográfica e documental, com base na doutrina especializada, legislação vigente e jurisprudência dos tribunais pátrios. Verificou-se que a dinamicidade das condutas virtuais, aliada à ausência de fronteiras territoriais no ciberespaço, dificultou a aplicação de normas tradicionais, impondo a necessidade de novas tipificações penais e instrumentos processuais mais céleres. Os resultados demonstraram que, embora a Lei nº 12.737/2012 e o Marco Civil da Internet tenham representado avanços significativos, ainda persistiram lacunas quanto à cooperação internacional, à responsabilização das plataformas digitais e à proteção efetiva dos direitos fundamentais dos usuários. Concluiu-se que a efetividade do combate aos crimes cibernéticos exigiu não apenas atualização legislativa, mas também integração entre os órgãos estatais e a sociedade civil, de modo a assegurar maior segurança jurídica e fortalecimento do Estado de Direito no ambiente digital.

Palavras-chave: crimes cibernéticos; implicações legais; era digital; segurança jurídica; cooperação internacional.

ABSTRACT

The study analyzed cybercrimes as an emerging legal phenomenon resulting from technological expansion and the increasing use of the internet in social and commercial relations. The objective was to understand the main challenges faced by the Brazilian legal system in repressing and preventing these illicit practices. The method adopted was bibliographical and documentary research, based on specialized doctrine, current legislation, and case law of national courts. It was found that the dynamic nature of virtual conduct, combined with the absence of territorial borders in cyberspace, hindered the application of traditional norms, imposing the need for new criminal classifications and faster procedural instruments. The results showed that, although Law No. 12.737/2012 and the Civil Rights Framework for the Internet represented significant progress, there were still gaps regarding international cooperation, the accountability of digital platforms, and the effective protection of users' fundamental rights. It was concluded that the effectiveness of combating cybercrimes required not only legislative updates but also integration between state institutions and civil society, in order to ensure greater legal security and strengthen the Rule of Law in the digital environment.

Keywords: cybercrimes; legal implications; digital age; legal security; international cooperation.

¹ Pontifícia Universidade Católica de Goiás, acadêmica de Direito.

INTRODUÇÃO

Nas últimas décadas, a sociedade vivenciou uma profunda transformação decorrente do avanço acelerado das tecnologias da informação e comunicação, consolidando o ambiente digital como espaço indispensável para o desenvolvimento das relações sociais, econômicas e institucionais, no entanto, juntamente com os inúmeros benefícios proporcionados pela internet e pelas novas tecnologias, surgiram também diversos riscos e vulnerabilidades, dentre os quais se destacam os crimes cibernéticos.

Os chamados crimes cibernéticos, também denominados delitos informáticos ou crimes digitais, configuram-se como práticas ilícitas cometidas por meio de sistemas informatizados, redes de computadores e dispositivos eletrônicos, com o objetivo de causar danos patrimoniais, morais ou institucionais, essas condutas abrangem desde fraudes bancárias e estelionatos virtuais até crimes mais complexos, como invasões de sistemas, disseminação de vírus, sequestro de dados, além de ataques contra órgãos públicos e infraestruturas críticas.

A era digital impôs desafios significativos ao Direito, que precisou se adaptar para oferecer respostas adequadas a um fenômeno caracterizado pela transnacionalidade, pelo anonimato dos agentes e pela volatilidade das provas, diante disso, o ordenamento jurídico brasileiro passou a incorporar legislações específicas voltadas à proteção do ambiente virtual, como o Marco Civil da Internet (Lei nº 12.965/2014), que estabelece princípios, garantias e deveres para o uso da rede; a Lei Carolina Dieckmann (Lei nº 12.737/2012), que tipifica condutas criminosas praticadas no meio digital; e a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), que assegura a privacidade e a segurança das informações pessoais dos cidadãos.

O problema central desta pesquisa consiste em analisar de que forma o sistema jurídico brasileiro tem se mostrado eficaz no enfrentamento dos crimes cibernéticos, considerando a complexidade das novas formas de criminalidade digital e a necessidade de garantir, simultaneamente, a proteção dos direitos fundamentais e a efetiva responsabilização dos infratores, nesse sentido, busca-se compreender se o atual arcabouço normativo e os instrumentos investigativos disponíveis são suficientes para combater de forma eficiente as condutas ilícitas praticadas no ambiente virtual.

O objetivo geral é examinar os principais desafios e implicações legais decorrentes dos crimes cibernéticos, com enfoque na realidade brasileira, mas sem desconsiderar a perspectiva internacional, uma vez que tais delitos frequentemente

ultrapassam fronteiras e demandam cooperação entre Estados, o estudo pretende, ainda, identificar as lacunas legislativas existentes, as dificuldades na responsabilização dos agentes e os desafios relacionados à utilização de tecnologias de vigilância digital, propondo alternativas e políticas públicas que contribuam para o aprimoramento da segurança jurídica no meio virtual.

A relevância do tema se justifica diante do crescimento exponencial dessas práticas ilícitas, que afetam não apenas indivíduos, mas também empresas e governos, gerando prejuízos econômicos, sociais e institucionais de grandes proporções, essas circunstâncias exigem uma atuação estatal coordenada e multidisciplinar, envolvendo não apenas o Direito Penal e Processual Penal, mas também o Direito Digital, o Direito Constitucional e o Direito Internacional.

Metodologicamente, a pesquisa adota uma abordagem dedutiva com base em revisão bibliográfica e análise documental, buscando compreender as complexidades que envolvem a tipificação penal, a investigação e a punição dos crimes cibernéticos, considerando as especificidades da era tecnológica.

A primeira parte do trabalho será dedicada a apresentar o histórico dos crimes cibernéticos no Brasil, demonstrando a evolução dessas práticas ilícitas e o surgimento de legislações voltadas à sua repressão, também serão abordados o conceito e a tipologia dos crimes digitais, com a análise de suas principais características e modalidades, desde os delitos contra o patrimônio até os crimes contra a honra e a privacidade no ambiente virtual.

Na sequência, a segunda parte da pesquisa abordará as lacunas legislativas existentes no ordenamento jurídico brasileiro, examinando a adequação das normas vigentes às novas formas de criminalidade digital, serão analisadas as dificuldades enfrentadas na responsabilização penal dos infratores, especialmente diante do caráter transnacional da internet e da necessidade de cooperação internacional. Além disso, discutir-se-ão os desafios éticos e jurídicos relacionados ao uso das tecnologias de vigilância digital, considerando o equilíbrio entre segurança pública e proteção de direitos fundamentais, como a privacidade e o sigilo das comunicações.

A terceira parte do estudo apresentará um caso concreto envolvendo fraude digital, que servirá como base empírica para demonstrar a aplicação das normas jurídicas no enfrentamento dos crimes cibernéticos e os obstáculos encontrados durante a persecução penal.

Nessa etapa, será analisada a responsabilidade penal dos agentes envolvidos e, ao final, serão discutidas as propostas de políticas públicas e estratégias de prevenção destinadas a combater os golpes cibernéticos e fortalecer a segurança digital no Brasil.

Dessa forma, o presente trabalho visa contribuir para o aperfeiçoamento do debate jurídico sobre os crimes cibernéticos, oferecendo uma análise crítica e sistematizada sobre as falhas e potencialidades do ordenamento jurídico brasileiro diante dos desafios da era digital, a expectativa é que o estudo proporcione subsídios teóricos e práticos que auxiliem na construção de um sistema normativo mais eficaz, justo e compatível com as transformações tecnológicas contemporâneas.

1. Secção I – O HISTÓRICO DOS CRIMES CIBERNÉTICOS NO BRASIL

A preocupação estatal com as chamadas condutas informáticas remonta à difusão da internet e das tecnologias das informações, nas últimas décadas do século XX, quando se começou a identificar, de modo sistemático, práticas que causavam danos patrimoniais e extrapatrimoniais por meios eletrônicos.

Desde então, foi necessário a adequação de normas penais e tradicionais, para enquadrar todas as condutas dessa nova feição tecnológica, desta forma nos anos 2000, com a massificação do acesso e o aumento exponencial de dados pessoais trafegados online, cresceram as formas de ilícitos desde fraudes bancárias e invasões de sistemas até difusão de material ilícito, o que impôs ao direito penal a necessidade de reagir por meio de tipificações específicas e reformas normativas.

Um marco inicial relevante no Brasil foi o reconhecimento da necessidade de tipificação de condutas como a invasão de dispositivo informático, que recebeu tratamento específico com a Lei nº 12.737/2012 conhecida popularmente como “Lei Carolina Dieckmann” ao criminalizar a invasão de dispositivo eletrônico para obtenção, adulteração ou destruição de dados.

Paralelamente, o debate sobre direitos e garantias no ambiente digital avançou para o campo civil e administrativo, materializando-se com o Marco Civil da Internet (Lei nº 12.965/2014), que consagrou princípios relativos à neutralidade, à proteção de dados e à responsabilização de intermediários, moldando o cenário em que a repressão aos crimes cibernéticos deveria operar.

Conforme o autor Lemos (2015, p.18), entende sobre o assunto:

A necessidade de tipificação penal clara e a construção de instrumentos processuais eficazes para investigação e cooperação, pois a natureza transfronteiriça dos delitos virtuais exige mecanismos de colaboração internacional e técnicas de investigação compatíveis com o ambiente digital.

No plano penal, a Lei nº 12.737/2012 e demais diplomas suscitaram debates doutrinários quanto à amplitude de seus tipos abstratos e à observância do princípio da legalidade penal, especialmente em face de tipos abertos ou em branco que deixam margem interpretativa para o julgador.

A resposta normativa, porém, não se limitou ao direito penal no campo administrativo e civil constataram-se esforços para regular a responsabilidade das leis civis das plataformas e provedores de serviços, equilibrando direitos fundamentais, como o da privacidade, liberdade de expressão e o dever de prevenção e colaboração com autoridades, questão que o Marco Civil procurou endereçar, ainda que sem esgotar a problemática.

Conforme o entendimento do autor Sanches (2023, p.4-12), entende:

A tutela dos dados pessoais ganhou reforço legislativo com a Lei Geral de Proteção de Dados (Lei nº 13.709/2018 — LGPD), que, embora não seja norma penal, engenhou novo arcabouço de proteção, obrigações e sanções administrativas que impactam diretamente o enfrentamento dos crimes cibernéticos e a reparação de vítimas.

A importância de políticas públicas integradas e de formação tecnológica das forças de investigação e do Poder Judiciário, apontando que a mera tipificação penal é insuficiente sem capacitação técnica, cooperação entre instituições e fluxos processuais aptos a preservar provas digitais.

Em paralelo, surgiram iniciativas legislativas posteriores que visaram agravar penas ou tipificar novas condutas, reflexo da percepção social e política sobre a grave lesividade de determinados delitos eletrônicos, contudo, a doutrina adverte para a necessidade de balanceamento entre repressão e garantias fundamentais, evitando soluções simplisticamente punitivas.

O histórico dos crimes cibernéticos no Brasil revela trajetória de avanços normativos importantes a Lei 12.737/2012; Marco Civil, LGPD, mas também evidencia lacunas institucionais e práticas que exigem políticas contínuas de cooperação internacional, capacitação técnica e diálogo entre legisladores, operadores do direito e sociedade civil, tais medidas são indispensáveis para que o ordenamento alcance eficácia na prevenção e repressão dos delitos em um ambiente tecnológico em constante mutação.

1.2 O CONCEITO E A TIPOLOGIA DOS CRIMES CIBERNÉTICOS

A criminalidade contemporânea apresenta novas formas de manifestação, especialmente com o advento das tecnologias da informação e comunicação, nesse contexto, os crimes cibernéticos surgem como uma expressão da modernização das práticas ilícitas, exigindo do ordenamento jurídico uma resposta eficaz.

Segundo Filho (2006, p. 47), afirma que:

Pode-se afirmar que esses delitos representam a adaptação da delinquência tradicional aos novos ambientes digitais, exigindo da legislação penal permanente atualização para garantir a efetividade da tutela jurídica, observa-se, portanto, que o conceito de crimes cibernéticos está diretamente ligado à evolução social e tecnológica.

Crespo (2012, p. 88) sustenta que:

Os crimes digitais não se restringem a figuras típicas inéditas, mas também abrangem práticas já conhecidas que se utilizam da rede como meio de execução, importante ressaltar que o autor, enfatiza que o ambiente virtual proporciona ao infrator uma sensação de anonimato e de dificuldade na persecução penal, o que torna esses delitos mais complexos de serem investigados, essa perspectiva permite compreender que os crimes cibernéticos exigem uma análise técnica e jurídica diferenciada, sob pena de ineficiência na repressão penal.

A criminalidade informática desafia os fundamentos tradicionais do Direito Penal, a natureza transnacional da internet cria impasses sobre competência jurisdicional, territorialidade e aplicação da lei penal no espaço, impondo aos Estados uma necessidade de cooperação internacional, essa análise revela que a tipologia dos crimes cibernéticos não pode ser compreendida apenas sob a ótica doméstica, mas deve dialogar com normas internacionais que buscam harmonizar as respostas penais.

Gomes (2013, p. 76) acrescenta que:

O enfrentamento dos crimes digitais deve ser visto como uma forma de proteção dos direitos fundamentais, a tipificação de condutas relacionadas à informática não constitui mero capricho legislativo, mas sim instrumento de preservação da privacidade, da honra, da segurança da informação e da dignidade da pessoa humana, assim, os crimes cibernéticos assumem relevância não apenas patrimonial, mas também na defesa de bens jurídicos de natureza existencial.

Os delitos de fraude eletrônica e práticas abusivas contra consumidores online demonstram que o espaço digital é marcado por profundas assimetrias, exigindo mecanismos específicos de proteção, essa perspectiva amplia a compreensão da tipologia dos crimes cibernéticos, incluindo não apenas os ataques diretos a sistemas, mas também práticas lesivas a consumidores.

Greco (2015, p. 211) propõe uma distinção relevante para a doutrina penal:

E possível dividir os crimes cibernéticos em duas categorias os próprios, que só podem ser praticados em ambiente digital, como invasões de sistemas, e os impróprios, nos quais a informática é apenas o meio de execução, como ocorre nas fraudes eletrônicas, essa classificação contribui para o aprimoramento da dogmática penal, permitindo uma aplicação mais precisa do direito.

O caráter transnacional desses delitos pode ser articulado de qualquer local do mundo, valendo-se de servidores internacionais, o que dificulta a persecução penal e a efetividade das decisões judiciais, a cooperação entre os Estados é elemento essencial, sobretudo em razão da adoção de tratados internacionais como a Convenção de Budapeste, que busca uniformizar práticas de combate ao cibercrime.

O autor Nucci (2018, p. 178) ressalta que o processo penal também enfrenta desafios específicos, afirma:

A coleta e a preservação da prova digital são extremamente frágeis, exigindo técnicas avançadas e confiáveis, sob pena de nulidade e comprometimento do devido processo legal, essa preocupação evidencia que, além da tipificação penal, a efetividade no enfrentamento dos crimes cibernéticos depende de inovações processuais e de garantias probatórias robustas.

O Direito Penal deveria se moldar às novas manifestações da criminalidade, a lei penal deve ser encarada como organismo dinâmico, apto a acompanhar o progresso social e as formas inovadoras de delinquência, embora contextualizada em outra época, a lição demonstra a atemporalidade da necessidade de adaptação normativa, princípio aplicável ao fenômeno do cibercrime.

Bottini (2020, p. 59) defende que a classificação dos crimes digitais não deve ater-se apenas à natureza formal da conduta, desta forma sustenta:

A gravidade do impacto social das práticas ilícitas em rede deve orientar a política criminal, considerando a rápida disseminação de informações e o alcance potencialmente irreversível dos danos, dessa forma, a tipologia deve considerar não só a estrutura do delito, mas também suas consequências sociais.

As redes sociais potencializaram condutas criminosas ligadas à honra, ao discurso de ódio e à disseminação de informações falsas, a ausência de uniformidade legislativa em diversos países provoca insegurança jurídica, permitindo que agentes explorem lacunas normativas para se beneficiar da impunidade, esse cenário revela a necessidade de reformas legislativas capazes de oferecer maior segurança jurídica frente às novas formas de criminalidade.

Portanto, que o conceito e a tipologia dos crimes cibernéticos se consolidam como tema indispensável à dogmática penal contemporânea, porém a doutrina converge

em afirmar que tais delitos exigem regulamentação constante e técnicas de investigação especializadas, a fim de garantir proteção eficaz aos direitos fundamentais na sociedade da informação, a complexidade do fenômeno evidencia que o enfrentamento dos crimes digitais não pode se limitar ao campo normativo, devendo ser acompanhado por cooperação internacional, inovação tecnológica e respeito às garantias constitucionais.

1.3 As Características e as Modalidades de Crimes Digitais

A sociedade da informação transformou não apenas a forma de comunicação, mas também a estrutura da criminalidade, nesse cenário, os crimes digitais passaram a representar uma nova face do fenômeno delitivo, marcada pela velocidade, alcance e dificuldade de repressão.

Para Filho (2006, p. 49), comenta que:

A criminalidade que se vale das tecnologias da informação possui como característica fundamental a transnacionalidade, rompendo fronteiras físicas e tornando ineficaz a tradicional delimitação territorial da lei penal, essa constatação evidencia que a natureza global da internet é um dos traços definidores das infrações digitais.

Os delitos cibernéticos se caracterizam também pela sensação de anonimato que envolve seus agentes, a rede mundial de computadores confere aos delinquentes a falsa percepção de invisibilidade, o que fomenta práticas ilícitas e dificulta a identificação dos autores, esse traço reforça a complexidade investigativa e coloca em xeque os mecanismos tradicionais de responsabilização penal.

Outro aspecto essencial é destacado por Greco (2014, p. 135), ao afirmar que:

A instantaneidade da propagação de informações ilícitas na internet constitui característica intrínseca dos crimes digitais, aumentando significativamente o potencial de danos causados à vítima e à coletividade.

A criminalidade digital não se limita a proteger bens patrimoniais, mas atinge direitos fundamentais, os crimes cometidos em meio eletrônico se diferenciam porque não apenas afetam a propriedade ou o patrimônio, mas alcançam diretamente a honra, a imagem, a privacidade e até mesmo a integridade psicológica das vítimas, isso demonstra que os delitos digitais possuem um caráter multifacetado, impactando bens jurídicos de natureza patrimonial e extrapatrimonial.

Marques (2019, p. 59) enfatiza a vulnerabilidade dos consumidores no ambiente eletrônico como traço marcante dos crimes digitais, desta forma afirma que:

As fraudes eletrônicas, as práticas abusivas de coleta de dados e os golpes em plataformas de comércio online revelam a assimetria de poder entre fornecedores e usuários, evidenciando a necessidade de maior proteção jurídica, sendo assim, a dimensão consumerista dos delitos digitais constitui uma modalidade relevante que merece destaque na tipologia.

Os crimes informáticos podem ser classificados em próprios, aqueles que só existem em ambiente digital, como a invasão de dispositivos, e impróprios, que utilizam a informática como meio para concretizar delitos tradicionais, como estelionato virtual, essa distinção auxilia na construção dogmática e permite que a legislação seja mais específica na tipificação.

Lima (2016, p. 404) acrescenta que os crimes digitais também se diferenciam pelo caráter descentralizado da prática criminosa, conforme o autor, afirma que:

O agente pode executar sua conduta em determinado país, utilizando servidores localizados em outro e atingindo vítimas em regiões distintas, o que torna a persecução penal dependente de acordos internacionais de cooperação, sendo assim, a modalidade desses delitos frequentemente envolve múltiplas jurisdições, desafiando os limites da lei penal no espaço.

Essa peculiaridade reforça a necessidade de inovação legislativa e tecnológica para enfrentar adequadamente tais condutas, as modalidades de crimes digitais devem ser analisadas não apenas sob o prisma técnico, mas também sob sua repercussão social.

A cada inovação tecnológica abre espaço para novas formas de criminalidade, exigindo constante atualização das categorias jurídicas e da legislação penal, essa observação reforça que a tipologia dos crimes digitais não é estática, mas dinâmica, acompanhando o ritmo acelerado das transformações sociais.

2. Seção II - AS LACUNAS LEGISLATIVAS NO ORDENAMENTO JURÍDICO BRASILEIRO

As lacunas legislativas constituem fenômeno inevitável nos sistemas jurídicos, uma vez que nenhuma norma é capaz de prever todas as situações possíveis da vida em sociedade.

Nesse sentido, Diniz (2001, p. 45) sustenta que:

A lei, sendo fruto da atividade humana, jamais poderá abranger todas as hipóteses da realidade, razão pela qual surgem lacunas que exigem do intérprete a busca de soluções dentro do próprio sistema jurídico.

O ordenamento jurídico é um sistema dinâmico, mas necessariamente limitado, no qual sempre haverá situações não previstas pelo legislador, cabendo ao aplicador recorrer a princípios e analogias para suprir as omissões, o jurista deve demonstrar que a completude absoluta das normas é uma utopia, e o papel do intérprete é justamente o de garantir coerência ao sistema, evitando que a ausência de previsão gere injustiças.

Reale (2002, p. 112) argumenta que as lacunas são inevitáveis porque a realidade social está em constante transformação, desta forma afirma que:

O direito positivo, ainda que bem elaborado, não consegue acompanhar a velocidade das mudanças sociais, de modo que surgem vazios normativos que só podem ser superados pela integração da norma jurídica, essa análise evidencia a necessidade de flexibilidade no ordenamento para que continue funcional e adaptável.

Bobbio (1995, p. 147) defende que a própria ideia de lacuna está associada à noção de sistema, para ele}:

E possível reconhecer a incompletude das normas quando determinadas condutas não encontram resposta adequada no ordenamento, o que obriga o intérprete a recorrer a mecanismos de integração como a equidade e os princípios gerais do direito, a reflexão bobbiana aponta que as lacunas não são defeitos absolutos, mas limites próprios da normatividade.

As lacunas legislativas no Brasil possuem particular relevância em razão da intensa produção normativa, sendo assim quanto maior a proliferação de leis, maior a possibilidade de contradições e omissões, o que gera insegurança jurídica e compromete a previsibilidade das decisões judiciais.

Em matéria constitucional, as lacunas podem comprometer a eficácia dos direitos fundamentais, se houver a ausência de regulamentação adequada de determinados dispositivos constitucionais faz com que direitos assegurados formalmente não possam ser exercidos na prática, revelando uma grave falha do legislador, sendo assim, as lacunas não são apenas técnicas, mas também políticas, comprometendo a concretização da cidadania.

De acordo com Mello (2004, p. 77), no âmbito do direito administrativo, as lacunas são particularmente problemáticas, desta forma aponta:

A inexistência de normas específicas acerca de determinadas matérias administrativas abre espaço para arbitrariedades e interpretações excessivamente discricionárias, que podem violar os princípios da legalidade e da impessoalidade, esse diagnóstico reforça a importância da clareza legislativa.

O papel do Judiciário se intensifica quando há lacunas no ordenamento, o silêncio da lei confere ao juiz maior margem interpretativa, o que, embora necessário, também abre espaço para ativismos judiciais que nem sempre se coadunam com a vontade democrática do legislador, essa reflexão indica o duplo risco das lacunas: a insegurança jurídica e o enfraquecimento da separação de poderes.

Para Barroso (2013, p. 203), as lacunas legislativas podem ser supridas legitimamente por meio da utilização dos princípios constitucionais, comenta sobre:

Em situações de ausência normativa, os princípios funcionam como vetores interpretativos, permitindo a realização de justiça e evitando a inefetividade da Constituição, essa perspectiva amplia o papel dos princípios como instrumentos de integração normativa.

Desta forma, as lacunas legislativas no ordenamento jurídico brasileiro representam um fenômeno inerente à limitação da atividade legislativa, tendo o jurista a missão de transformar o silêncio normativo em oportunidade para a concretização da justiça, sem comprometer a coerência e a legitimidade do sistema.

2.2 AS DIFICULDADES NA RESPONSABILIZAÇÃO DOS INFRATORES

A responsabilização dos infratores constitui um dos maiores desafios contemporâneos do Direito Penal e Processual Penal, especialmente em se tratando de condutas praticadas em ambientes complexos, como o digital.

Segundo Greco (2014, p. 142), aduz que:

O processo de responsabilização encontra entraves na identificação do autor da conduta, na produção de provas válidas e na fixação da competência jurisdicional, problemas que se tornam ainda mais graves quando os delitos são praticados pela internet, a análise do autor evidencia a intersecção entre limites técnicos e jurídicos que dificultam a punição.

Os obstáculos que se relacionam, sobretudo, à ausência de uniformidade legislativa e à carência de mecanismos internacionais eficazes, a criminalidade, ao se tornar transnacional, desafia as fronteiras jurídicas estatais, gerando impunidade em razão da dificuldade de cooperação entre países, que muitas vezes não dispõem de tratados comuns sobre determinadas práticas ilícitas, essa perspectiva revela que a responsabilização dos infratores não depende apenas de leis nacionais, mas de integração global.

De acordo com Lima (2016, p. 410), determina que:

A responsabilização criminal enfrenta sérias dificuldades em razão da volatilidade das provas digitais, as quais podem ser facilmente apagadas,

adulteradas ou armazenadas em servidores estrangeiros, a fragilidade da prova compromete a materialidade do delito e, conseqüentemente, a persecução penal, impondo aos órgãos estatais a adoção de técnicas modernas de investigação.

A questão da responsabilização também esbarra na necessidade de respeitar as garantias fundamentais, desta forma a obtenção de provas por meios ilícitos ou invasivos não pode ser admitida, sob pena de comprometer o devido processo legal, mesmo que isso dificulte a punição do infrator, essa análise demonstra a tensão entre eficiência investigativa e preservação dos direitos constitucionais, dificultando ainda mais a responsabilização.

Marques (2019, p. 65) observa que, no campo das relações de consumo, as dificuldades se agravam, pois:

Os consumidores vítimas de fraudes digitais enfrentam barreiras jurídicas e práticas para identificar os responsáveis e obter reparação, já que muitas vezes os autores ocultam-se sob falsas identidades ou utilizam-se de meios tecnológicos para encobrir rastros, a autora chama atenção para a vulnerabilidade da parte hipossuficiente frente à sofisticação dos métodos ilícitos.

A dificuldade de responsabilizar infratores está ligada ao caráter descentralizado da internet, os agentes ao praticarem atos ilícitos a partir de qualquer localidade, utilizando servidores situados em diferentes jurisdições, o que fragmenta a investigação e impede respostas rápidas e coordenadas, essa constatação evidencia a dependência de cooperação internacional para a efetividade do direito penal no espaço digital.

Bobbio (1995, p. 152), em reflexão clássica sobre a aplicação das normas, já afirmava que:

A dificuldade de responsabilizar infratores decorre não apenas das lacunas normativas, mas também da insuficiência prática dos mecanismos de aplicação, que muitas vezes se mostram ineficazes diante da realidade social, embora anterior ao contexto digital, a análise permanece atual, pois evidencia a distância entre a norma abstrata e sua efetividade concreta.

A lentidão da justiça faz com que, mesmo quando identificado e processado, o infrator se beneficie da prescrição ou de recursos intermináveis, o que compromete a efetividade da sanção penal, essa crítica ressalta que os obstáculos não são apenas técnicos, mas também estruturais, ligados à máquina judiciária.

As dificuldades na responsabilização dos infratores colocam em risco a própria legitimidade do Estado Democrático de Direito, levando a incapacidade estatal

de dar respostas adequadas às práticas ilícitas mina a confiança social nas instituições e favorece a sensação de impunidade, corroendo os fundamentos da ordem jurídica.

Os princípios constitucionais devem ser os norteadores na superação das dificuldades de responsabilização, a interpretação constitucional pode oferecer soluções criativas para suprir lacunas normativas e garantir a efetividade do sistema, desde que preservados os direitos fundamentais e a proporcionalidade das medidas, sendo assim, ainda que complexa, a responsabilização dos infratores deve ser perseguida como forma de assegurar justiça e efetividade ao ordenamento jurídico.

2.3 Os Desafios no Uso das Tecnologias da Vigilância Digital

O avanço das tecnologias de vigilância digital trouxe relevantes ferramentas para a segurança pública e para o combate ao crime, mas também levantou sérias preocupações jurídicas.

De acordo com Greco (2014, p. 150), comenta que:

A utilização de meios digitais de monitoramento exige análise criteriosa, pois, embora representem instrumentos de eficiência na persecução penal, também podem comprometer direitos fundamentais, como a intimidade e a privacidade, essa ponderação mostra que o maior desafio é conciliar eficácia e garantias constitucionais.

O uso indiscriminado de tecnologias de vigilância pode significar um retrocesso democrático, a expansão da vigilância estatal sem o devido controle judicial coloca em risco os princípios do Estado de Direito, transformando medidas legítimas de investigação em mecanismos de opressão e abuso de poder.

Lima (2016, p. 415) aponta que a coleta de dados digitais para fins de investigação enfrenta o desafio da legalidade estrita, em suas palavras:

É imprescindível que a utilização de tecnologias de monitoramento esteja amparada em lei específica e sujeita à autorização judicial, sob pena de nulidade das provas e violação do devido processo legal, essa perspectiva reforça a importância de que a vigilância digital seja utilizada dentro de parâmetros jurídicos seguros.

Outro desafio é a confiabilidade técnica das ferramentas digitais, o risco de manipulação ou falhas em softwares de vigilância levanta dúvidas sobre a autenticidade das informações coletadas, de modo que sua utilização no processo penal deve ser acompanhada de perícias especializadas e rígidos critérios de admissibilidade, essa observação ressalta que a tecnologia, embora útil, não é infalível e exige controle rigoroso.

O monitoramento digital também afeta diretamente os consumidores, a coleta massiva de dados pessoais para fins comerciais ou de vigilância compromete a autodeterminação informativa dos cidadãos, criando um cenário em que a privacidade se torna mercadoria e o indivíduo, vulnerável às práticas abusivas.

Greco (2015, p. 225) chama a atenção para o caráter transnacional das tecnologias de vigilância, ele explica que:

Os dados coletados muitas vezes são armazenados em servidores situados no exterior, criando um conflito de jurisdições e dificultando o controle estatal sobre o uso dessas informações, isso mostra que o desafio da vigilância digital ultrapassa as fronteiras nacionais, exigindo cooperação internacional e regulamentações conjuntas.

O poder de controle do Estado, se não limitado, poderia ameaçar liberdades individuais, a multiplicação dos instrumentos de observação e monitoramento, quando utilizados sem limites democráticos, tende a consolidar um modelo de Estado vigilante, no qual a vida privada se torna permanentemente exposta.

O caminho para enfrentar os desafios da vigilância digital está na constitucionalização da proteção de dados, e na autodeterminação informativa devem ser tratadas como direitos fundamentais, garantindo ao cidadão instrumentos jurídicos eficazes contra abusos do poder público e do setor privado, dessa forma, o equilíbrio entre vigilância e direitos fundamentais se mostra indispensável à preservação do Estado Democrático de Direito.

3.Secção III – CASO CONCRETO O ESCÂNDALO CAMBRIDGE ANALYTICA

O avanço tecnológico trouxe inúmeros benefícios sociais, mas também originou novas modalidades delitivas, em especial no campo digital, os golpes cibernéticos assumem protagonismo entre as práticas ilícitas, atingindo tanto pessoas físicas quanto jurídicas, com graves impactos econômicos e sociais, nesse sentido, a doutrina destaca que a criminalidade virtual exige atualização constante do ordenamento jurídico, pois os meios de execução variam de acordo com a evolução tecnológica.

Conforme observa Blum (2018, p. 77), apontam que:

Os crimes cibernéticos não se restringem ao ambiente digital como um mero espaço de prática delitiva, mas representam um desafio ao sistema jurídico, uma vez que não respeitam fronteiras físicas e atingem vítimas de forma difusa, criando obstáculos à persecução penal e demandando cooperação internacional, essa perspectiva amplia a compreensão de que os golpes digitais não são apenas delitos isolados, mas fenômenos de natureza transnacional que desafiam a soberania dos Estados.

Um dos exemplos concretos mais recorrentes são os golpes de phishing, em que o agente induz a vítima a fornecer dados sensíveis sob a aparência de uma comunicação legítima, sobre o tema, Pinheiro (2020, p. 132) afirma que:

A engenharia social é o elemento central da maior parte dos golpes virtuais, pois explora a vulnerabilidade psicológica da vítima, conduzindo-a a um erro voluntário que resulta na entrega de suas próprias informações, a sofisticação dessas práticas coloca em xeque o nível de proteção jurídica disponível atualmente no Brasil.

Um caso bastante conhecido em 2018 veio à tona o escândalo Cambridge Analytica, no qual dados pessoais de dezenas de milhões de usuários do Facebook foram coletados de forma indevida pelo aplicativo *thisisyourdigitallife*, e utilizados para fins políticos, o caso suscitou intensa discussão internacional sobre proteção de dados, consentimento expresso e responsabilidade civil das plataformas digitais

No Brasil, o Departamento de Proteção e Defesa do Consumidor (DPDC) abriu processos administrativos contra o Facebook Inc. e Facebook Serviços Online do Brasil Ltda., investigando práticas abusivas no fornecimento de serviços, violação dos princípios de boa-fé, privacidade e informação clara ao consumidor.

Do ponto de vista penal, embora a conduta não tenha sido tipificada na sua totalidade como novo tipo penal específico, há debate sobre a aplicação de estelionato digital e fraude eletrônica, com base na Lei nº 14.155/2021, que agravou as penas para delitos praticados eletronicamente, acresce-se a tipificação de estelionato previsto no art. 171 do Código Penal, com as hipóteses previstas no §2º-A, para uso de meios eletrônicos ou fraudulentos.

Como doutrina de apoio, Marques (2007, p.1) enfatiza que:

No comércio eletrônico o princípio da confiança é abonado por fenômenos da virtualidade despersonalização, temporalidade, internacionalidade o que gera vulnerabilidade do consumidor, nesse sentido, a violação de expectativas legítimas, inclusive quanto à privacidade e integridade dos dados, abala a confiança necessária nas relações de consumo.

No âmbito processual, há necessidade de provas digitais e perícias técnicas para demonstrar como os dados foram coletados, quem teve acesso, se houve consentimento válido e claro, se o usuário foi induzido ao erro, a prova pericial digital torna-se elemento central em demandas judiciais com base em relações de consumo ou responsabilidade civil.

Em face dos elementos, pode-se afirmar que houve ofensa ao direito fundamental à privacidade, previsto na Constituição Federal no art. 5º, X, bem como ofensa à proteção de dados pessoais, com reflexos na Lei Geral de Proteção de Dados

(Lei nº 13.709/2018), o caso Cambridge Analytica evidencia inobservância de princípios como finalidade, transparência, consentimento, segurança.

Quanto à ação penal, conforme doutrina recente, a aplicação do §2º-A do art. 171 do Código Penal, introduzido pela Lei 14.155/2021, pressupõe o uso de redes sociais, contato telefônico, e-mail ou similar, para induzir ou manter a vítima em erro, o que se ajusta ao *modus operandi* observado nos casos de coleta indevida de dados com finalidade política ou de manipulação.

No campo civil, cabe indenização por danos morais e materiais tanto ao titular dos dados quanto ao consumidor e vítima que sofrer prejuízos decorrentes do uso indevido desses dados, e também pode incidir a responsabilidade das plataformas sob o Código de Defesa do Consumidor, especialmente nos artigos que tratam da prestação de serviço seguro, informação adequada e positiva, e da qualidade e segurança dos serviços oferecidos, a transparência no processo de coleta e uso de dados pessoais é dever legal e contratual.

Em termos doutrinários, Gonzaga (2023) trata:}

A juridicidade e regulamentação de técnicas de interface digital os *dark patterns* que embora não sejam idênticos ao escândalo Cambridge Analytica, ilustram como artifícios sutis de design podem induzir usuários ao erro, afetando seu consentimento, o que se aproxima do uso estratégico de dados pessoais para influenciar comportamento, sobretudo em ambientes de redes sociais.

Diante da multiplicidade de atores usuário, plataforma, coletor de dados, contratantes, cabe ainda o princípio da responsabilização múltipla ou solidária, principalmente quando não for possível distinguir atuação entre os diversos envolvidos, ou quando a falha de segurança de um se vincula diretamente à ação do outro, como nos termos do Marco Civil da Internet.

Outra modalidade de golpe cibernético que ganhou notoriedade é o chamado “golpe do WhatsApp”, no qual criminosos se passam por conhecidos da vítima para solicitar transferências, para Doneda (2019, p. 289), afirma que:

O problema não se reduz à fraude em si, mas à insuficiência de mecanismos de autenticação e proteção de identidade nos aplicativos de mensagens, o que gera questionamentos quanto à responsabilidade compartilhada entre usuários, provedores e plataformas digitais, esse cenário reforça a necessidade de aprimorar a regulação setorial e de implementar padrões técnicos de segurança.

No plano penal, observa-se a dificuldade de tipificação específica para algumas condutas, embora o Código Penal tenha sofrido alterações, ainda há lacunas, de acordo com Crespo (2017, p. 164) destaca que:

A ausência de tipos penais claros e atualizados gera insegurança jurídica, favorecendo a impunidade, muitos golpes virtuais acabam sendo enquadrados de forma genérica em estelionato, o que não reflete adequadamente a complexidade e a gravidade das condutas praticadas, sendo assim, a evolução legislativa mostra-se imprescindível.

No campo internacional, observa-se que a cooperação entre Estados é elemento essencial para combater esses crimes, de acordo com Marinoni (2021, p. 299) enfatiza que:

A atuação isolada das jurisdições nacionais é insuficiente para enfrentar a criminalidade digital, a cooperação jurídica internacional constitui mecanismo indispensável para a efetividade da investigação, pois os dados estão dispersos em provedores situados em múltiplos territórios, esse fator evidencia que o combate a golpes cibernéticos requer uma abordagem global.

Além disso, a educação digital preventiva surge como um dos instrumentos mais eficazes contra esses delitos, a legislação, por si só, não é capaz de prevenir os golpes cibernéticos, é necessário investir em programas contínuos de conscientização digital, de forma a reduzir a vulnerabilidade da população, a informação constitui o antídoto mais eficiente contra a manipulação psicológica empregada pelos criminosos digitais.

Portanto, os casos concretos de golpes cibernéticos demonstram a urgência de uma resposta jurídica multifacetada, que envolva não apenas a atualização legislativa, mas também a responsabilização civil e penal adequada, a cooperação internacional e a promoção da educação digital, o Direito deve adaptar-se à realidade tecnológica para cumprir sua função primordial de garantir segurança e justiça às vítimas do ambiente virtual.

3.2 A RESPONSABILIDADE PENAL DOS AGENTES

A responsabilidade penal dos agentes em crimes cibernéticos constitui um dos temas mais complexos do Direito Penal contemporâneo, uma vez que envolve a aplicação de normas tradicionais a um ambiente inovador e mutável como o digital.

Conforme comenta Greco (2014, p. 143) adverte que:

A identificação da autoria em crimes virtuais é permeada por dificuldades técnicas que não se observam em delitos convencionais, o que demanda novas estratégias investigativas e interpretativas para que a imputação penal seja justa e eficaz, dessa forma, verifica-se que a responsabilização não se limita à tipicidade formal, mas exige também análise prática da dinâmica tecnológica.

Essa constatação demonstra que a legislação vigente precisa ser aplicada com cautela para evitar lacunas na proteção penal, de acordo com Crespo (2012, p. 95),

os crimes informáticos possuem peculiaridades que desafiam os institutos tradicionais do Direito Penal:

O agente pode atuar de forma anônima, em rede descentralizada, e ainda utilizar identidades falsas, o que dificulta o estabelecimento da autoria e, por consequência, a responsabilização penal. Assim, torna-se necessário repensar a interpretação jurídica frente às novas práticas delitivas.

O que se exige é a criação de normas claras e específicas que deem segurança jurídica à persecução penal, essa visão reforça a necessidade de equilíbrio entre combate à criminalidade e preservação de direitos fundamentais, importante ressaltar que segundo Gomes (2013, p. 100), a responsabilidade dos agentes deve observar estritamente o princípio da legalidade, ele enfatiza que “não é admissível ampliar, por analogia, a incidência de tipos penais a condutas praticadas no meio digital, sob pena de violação de garantias constitucionais.

Ao tratar da legalidade em crimes cibernéticos, certos tipos penais abertos ou em branco cria insegurança jurídica e compromete a responsabilização dos agentes, já que a norma penal deve ser suficientemente precisa para permitir ao indivíduo compreender a ilicitude de sua conduta, nesta análise revela que a imprecisão legislativa é fator determinante para a dificuldade de punir adequadamente os infratores.

Menke (2017, p. 64) também alerta para o problema da responsabilidade civil e penal dos provedores de internet, ele argumenta que:

Atribuir responsabilidade penal a intermediários que não participaram diretamente da conduta criminoso pode significar violação ao princípio da personalidade da pena, mas, ao mesmo tempo, a ausência de regras claras pode favorecer a impunidade, essa posição evidencia os dilemas entre imputação justa e eficácia na prevenção de delitos digitais.

A responsabilidade penal em crimes cibernéticos exige ainda o respeito ao devido processo legal, especialmente no tocante às provas, a volatilidade das informações digitais impõe grande desafio à comprovação da autoria e materialidade, tornando indispensável a adoção de procedimentos técnicos de coleta e cadeia de custódia digital para garantir a validade das provas, dessa forma, a responsabilização dos agentes depende não apenas da lei, mas também da técnica forense.

A governança da internet, traz a construção de um marco regulatório equilibrado é fundamental para que a responsabilidade penal dos agentes seja aplicada de forma justa, transparente e eficaz, sem desestimular o desenvolvimento tecnológico e a liberdade digital, desse modo, percebe-se que a responsabilização penal nos crimes

cibernéticos não pode ser pensada de forma isolada, mas integrada ao desenvolvimento da sociedade da informação.

3.3. As Propostas de Políticas Públicas para Combater os Golpes Cibernéticos

O enfrentamento dos golpes cibernéticos exige mais do que a atuação repressiva do Estado, demanda a formulação de políticas públicas que previnam, eduquem e promovam segurança no ambiente digital.

Segundo Bottini (2020, p. 92), expõe:

A criminalidade virtual apresenta características de difusão em massa e baixo custo para o infrator, o que exige do poder público estratégias de prevenção integradas, pautadas na educação digital da população e em medidas de fortalecimento da capacidade investigativa estatal, dessa forma, o combate deve ser estruturado em eixos múltiplos, e não apenas na esfera penal.

O autor afirma que a educação é a principal barreira contragolpes, pois capacita o indivíduo a identificar fraudes e adotar posturas de autoproteção, diminuindo a vulnerabilidade que os criminosos exploram, nesse contexto, a prevenção assume papel central, reduzindo a dependência de medidas repressivas, Crespo (2012, p. 110), políticas públicas voltadas à criminalidade virtual precisam contemplar a inclusão de disciplinas sobre cidadania digital nos currículos escolares.

As políticas públicas eficazes devem estar alinhadas com o princípio da legalidade e da proporcionalidade, a elaboração normativa não pode ser casuística ou emergencial, mas deve surgir de um planejamento que considere a natureza mutável dos crimes digitais, evitando a edição de leis desatualizadas ou ineficazes, essa visão demonstra que o enfrentamento de golpes cibernéticos depende de legislação clara, mas também de políticas flexíveis e adaptáveis.

Segundo Grokskreutz (2024, p. 15), a insegurança jurídica é um dos maiores obstáculos ao combate aos crimes digitais:

A vagueza normativa de certos tipos penais compromete a atuação estatal, de modo que políticas públicas devem priorizar a atualização constante da legislação, acompanhando os avanços tecnológicos e garantindo segurança jurídica tanto para o acusado quanto para a vítima, essa análise ressalta a importância de mecanismos de atualização legislativa contínua.

A formulação das políticas públicas deve ser construída em diálogo com a sociedade civil, empresas e órgãos estatais, a fim de garantir legitimidade, transparência e eficácia no enfrentamento da criminalidade digital, os autores evidenciam que a

atuação isolada do Estado não é suficiente, sendo indispensável um modelo cooperativo para combater fraudes online.

Para Menke (2017, p. 72), a responsabilização dos provedores também deve ser considerada nas políticas públicas, ele sustenta que:

Embora não se possa transferir ao intermediário a responsabilidade penal por golpes praticados por terceiros, é possível e necessário estabelecer mecanismos de colaboração obrigatória, sobretudo quanto ao fornecimento rápido de dados que auxiliem na identificação dos infratores, essa proposta busca equilibrar liberdade empresarial e dever de cooperação.

O combate ao crime não pode justificar a violação da intimidade e da privacidade, sob pena de transformar a vítima em novo alvo de abuso estatal, é necessário que as medidas respeitem os princípios constitucionais e mantenham o equilíbrio entre segurança e liberdade, sendo assim, conclui-se que o enfrentamento dos golpes cibernéticos precisa de políticas públicas abrangentes, que integrem prevenção, repressão, cooperação internacional e proteção de direitos.

CONCLUSÃO

A era digital trouxe consigo um avanço tecnológico sem precedentes, ampliando o acesso à informação, à comunicação e à conectividade, no entanto, esse mesmo ambiente virtual também se transformou em terreno fértil para práticas ilícitas, como fraudes eletrônicas, invasões de sistemas, disseminação de dados pessoais e crimes contra a honra, essas condutas demonstram que o progresso tecnológico, embora essencial, exige mecanismos jurídicos cada vez mais sofisticados para acompanhar a evolução das ameaças cibernéticas.

Os crimes cibernéticos apresentam peculiaridades que os diferenciam das infrações tradicionais, a ausência de barreiras geográficas, o anonimato proporcionado pela internet e a dificuldade de rastreamento dos agentes tornam a persecução penal mais complexa, dessa forma, o sistema jurídico brasileiro enfrenta o desafio de equilibrar a proteção dos direitos fundamentais com a necessidade de repressão eficiente das condutas ilícitas digitais.

A Lei nº 12.737/2012, conhecida como “Lei Carolina Dieckmann”, e o Marco Civil da Internet (Lei nº 12.965/2014) representam avanços significativos no combate aos delitos virtuais, contudo, a velocidade com que as tecnologias evoluem faz com que tais legislações se tornem, em muitos aspectos, insuficientes. É imprescindível que o

ordenamento jurídico seja constantemente atualizado, de modo a abranger novas modalidades de crime digital, como ataques de ransomware, deepfakes e fraudes com criptomoedas.

Outro aspecto relevante é a cooperação internacional, os crimes cibernéticos, em sua maioria, ultrapassam fronteiras nacionais, exigindo um esforço conjunto entre países para investigação, coleta de provas e punição dos infratores, a adesão do Brasil à Convenção de Budapeste sobre Cibercrime, ainda em debate, seria um passo importante para fortalecer a cooperação jurídica internacional e aprimorar a eficácia do combate global às ameaças virtuais.

A atuação do Poder Judiciário e das autoridades de investigação precisa ser pautada pela especialização técnica, o treinamento de policiais, peritos e membros do Ministério Público é fundamental para compreender a dinâmica dos crimes digitais e empregar métodos adequados de rastreamento e coleta de evidências eletrônicas, a ausência de capacitação específica pode comprometer a efetividade da persecução penal e, consequentemente, a confiança da sociedade na justiça.

Paralelamente, é necessário fortalecer políticas públicas voltadas à educação digital e à conscientização da população, grande parte dos crimes cibernéticos ocorre em razão da falta de conhecimento dos usuários sobre práticas seguras na internet, as campanhas educativas, programas escolares e parcerias entre governo e setor privado podem contribuir para a formação de uma cultura de segurança cibernética mais sólida e preventiva.

Do ponto de vista jurídico, os desafios também incluem a definição de limites entre a liberdade de expressão e a responsabilização por danos causados no ambiente virtual, o discurso de ódio, a desinformação e os ataques à reputação são exemplos de condutas que exigem um tratamento cuidadoso, a fim de preservar tanto os direitos individuais quanto a integridade das relações sociais no ciberespaço.

A proteção de dados pessoais, especialmente após a vigência da Lei Geral de Proteção de Dados (Lei nº 13.709/2018), assume papel central nesse contexto, o tratamento inadequado de informações sensíveis pode gerar prejuízos econômicos, morais e sociais, sendo assim, as empresas e instituições públicas devem adotar medidas técnicas e administrativas eficazes para garantir a segurança da informação, sob pena de sanções legais e danos à reputação.

O avanço da inteligência artificial e das tecnologias emergentes, como o metaverso e a internet das coisas, amplia ainda mais o campo de atuação dos crimes cibernéticos, essas inovações trazem novas oportunidades, mas também riscos inéditos, o legislador, portanto, precisa antecipar-se a essas transformações, criando marcos regulatórios flexíveis e capazes de responder rapidamente às demandas da sociedade digital.

E igualmente importante destacar a responsabilidade das plataformas digitais. Redes sociais, provedores de acesso e empresas de tecnologia devem adotar mecanismos de monitoramento, denúncia e remoção de conteúdos ilícitos, em conformidade com as normas vigentes e respeitando o devido processo legal, o combate aos crimes cibernéticos não pode depender exclusivamente do Estado, devendo envolver todos os atores da sociedade digital.

Os crimes cibernéticos representam um dos maiores desafios jurídicos da contemporaneidade, sua complexidade exige uma abordagem multidisciplinar, integrando direito, tecnologia, segurança da informação e educação, somente por meio de uma atuação coordenada será possível reduzir a impunidade, proteger os cidadãos e preservar a confiança nas relações digitais.

Portanto, a efetividade do enfrentamento aos crimes cibernéticos depende da constante atualização das leis, da especialização das instituições e da conscientização coletiva, o direito deve acompanhar o ritmo da inovação tecnológica, garantindo que o progresso digital ocorra de forma ética, segura e compatível com os valores fundamentais do Estado Democrático de Direito, sendo assim, a sociedade poderá usufruir plenamente dos benefícios da era digital, sem se tornar refém de seus riscos.

REFERÊNCIAS BIBLIOGRÁFICAS

ARAÚJO, C. R. Crimes-virtuais: tipificações e desafios. Expert Editora, 2023. Disponível em: <https://experteditora.com.br/wp-content/uploads/2023/07/Crimes-virtuais.pdf>. Acesso em: 24/09/2025.

BARROSO, Luís Roberto. Curso de Direito Constitucional Contemporâneo. 5. ed. São Paulo: Saraiva, 2013.

BOBBIO, Norberto. Teoria do Ordenamento Jurídico. 6. ed. Brasília: Editora UnB, 1995.

BONAVIDES, Paulo. Curso de Direito Constitucional. 12. ed. São Paulo: Malheiros, 2001.

BOTTINI, Pierpaolo. Crimes cibernéticos e sociedade da informação. São Paulo: Revista dos Tribunais, 2020.

CAMPOS, F. C. A. da Silva. A Lei Carolina Dieckmann e o combate aos crimes virtuais. Gran Cursos Online periódico, 2025. Disponível em: <https://periodicos.grancursosonline.com.br/granic/article/view/18>. Acesso em: 24/09/2025.

CRESPO, Marcelo. Crimes de informática. São Paulo: Saraiva, 2012.

CLÁUDIA LIMA MARQUES. Direitos do Consumidor no Comércio Eletrônico. São Paulo: Editora RT, 2007.

DINIZ, Maria Helena. Lacunas do Direito. 7. ed. São Paulo: Saraiva, 2001.

FERRAZ JÚNIOR, Tércio Sampaio. Introdução ao Estudo do Direito: técnica, decisão e dominação. 5. ed. São Paulo: Atlas, 2003.

FERREIRA FILHO, Manoel Gonçalves. Curso de Direito Constitucional. 34. ed. São Paulo: Saraiva, 2006.

GONZAGA, Heitor Ferreira. *A Juridicidade e a Regulamentação dos Dark Patterns*. 2023. Disponível em: arXiv.

GOMES, Luiz Flávio. Direito penal aplicado: crimes cibernéticos. São Paulo: Revista dos Tribunais, 2013.

GRECCO, Rogério. Título genérico sobre estelionato digital e tipos de crimes virtuais. 2022.

GROKSKREUTZ, Hugo Rogério. Os crimes cibernéticos e o princípio da legalidade: os tipos penais abertos, em branco e a indefinição de dispositivos informáticos. Revista Brasileira de Ciências Criminais — RBCCRIM, 2024. Disponível em: <https://publicacoes.ibccrim.org.br/index.php/RBCCRIM/article/view/86>. Acesso em: 22/09/2025.

GRECO, Marco Aurélio. Direito e Internet: aspectos jurídicos relevantes. São Paulo: Dialética, 2015.

GRECO, Rogério. Direito Penal do Equilíbrio. 10. ed. Rio de Janeiro: Impetus, 2014.

HUNGRIA, Nelson. Comentários ao Código Penal. Rio de Janeiro: Forense, 1958.

LE MOS, Ronaldo; BLUM, Renato Opice. Debates sobre a governança da internet, Marco Civil e responsabilidades. Publicações e apresentações (selecionadas), 2015–2020.

LIMBERGER, Têmis. Cibertransparência: Informação Pública em Rede – A Virtualidade e Suas Repercussões na Realidade. Porto Alegre: Edições, ano de publicação conforme obra, p. conforme edição.

LIMA, Renato Brasileiro de. Legislação Penal Especial Comentada. Salvador: Juspodivm, 2016.

MARQUES, Cláudia Lima. Contratos no Código de Defesa do Consumidor. 8. ed. São Paulo: Revista dos Tribunais, 2019.

MELLO, Celso Antônio Bandeira de. Curso de Direito Administrativo. 16. ed. São Paulo: Malheiros, 2004.

MENKE, Fabiano. Direito e Internet: responsabilidade civil e penal. Porto Alegre: Livraria do Advogado, 2017.

NUCCI, Guilherme de Souza. Manual de Direito Penal. 14. ed. Rio de Janeiro: Forense, 2018.

REALE, Miguel. Lições Preliminares de Direito. 27. ed. São Paulo: Saraiva, 2002.

SILVA, José Afonso da. Curso de Direito Constitucional Positivo. 32. ed. São Paulo: Malheiros, 2010.

(Coletânea) Marco Civil da Internet: construção e aplicação. Instituto Tecnologia & Sociedade — ITS Rio; edição 2017. PDF disponível em: https://itsrio.org/wp-content/uploads/2017/02/marco_civil_construcao_aplicacao.pdf. Acesso em: 22/09/2025

(Artigo) Crimes cibernéticos / cyber crimes — Repositório Grupo Integrado, 2022. Disponível em: <https://repositorio.grupointegrado.br/index.php/rgi/catalog/download/74/76/197?inline=1>. Acesso em: 21/09/2025.