UNIVERSIDADE CESUMAR - UNICESUMAR
CENTRO DE CIÊNCIAS HUMANAS E SOCIAIS APLICADAS
CURSO DE GRADUAÇÃO EM DIREITO

INVESTIGAÇÃO CRIMINAL DIGITAL: OS DESAFIOS DA POLÍCIA JUDICIÁRIA NO COMBATE AOS CRIMES CIBERNÉTICOS

GUSTAVO HENRIQUE VENÁ DE OLIVEIRA

MARINGÁ – PR
2025

Gustavo Henrique Vená de Oliveira

INVESTIGAÇÃO CRIMINAL DIGITAL: OS DESAFIOS DA POLÍCIA JUDICIÁRIA NO COMBATE AOS CRIMES CIBERNÉTICOS

Artigo apresentado ao Curso de Graduação em _____ da Universidade Cesumar – UNICESUMAR como requisito parcial para a obtenção do título de Bacharel(a) em DIREITO, sob a orientação do Prof. Dr. Murilo Alan Volpi.

MARINGÁ – PR

2025

FOLHA DE APROVAÇÃO

GUSTAVO HENRIQUE VENÁ DE OLIVEIRA

INVESTIGAÇÃO CRIMINAL DIGITAL: OS DESAFIOS DA POLÍCIA JUDICIÁRIA NO COMBATE AOS CRIMES CIBERNÉTICOS

Artigo apresentado ao Curso de Graduação em DIREITO da Universidade Cesumar – UNICESUMAR como requisito parcial para a obtenção do título de Bacharel(a) em _____, sob a orientação do Prof. Dr. Murilo Alan Volpi.

Aprovado em: ____ de _____ de _____.

BANCA EXAMINADORA

_____

Nome do professor – (Titulação, nome e Instituição)

_____

Nome do professor - (Titulação, nome e Instituição)

_____

Nome do professor - (Titulação, nome e Instituição)

INVESTIGAÇÃO CRIMINAL DIGITAL: OS DESAFIOS DA POLÍCIA JUDICIÁRIA NO COMBATE AOS CRIMES CIBERNÉTICOS

Nome(s) do(s) autor(es): Gustavo Henrique Vená de Oliveira

RESUMO

A presente pesquisa tem como objetivo analisar criticamente a estrutura atual do Estado brasileiro no combate aos crimes cibernéticos, bem como investigar as principais dificuldades enfrentadas pelas polícias judiciárias na apuração de delitos cometidos no ambiente digital. O estudo adota o método dedutivo, baseado na análise de legislações, decretos e tratados internacionais relacionados ao tema. São examinados os avanços normativos e institucionais que fortalecem a atuação das autoridades investigativas, com destaque para a Lei nº 12.737/2012 (Lei Carolina Dieckmann) e para a incorporação da Convenção de Budapeste ao ordenamento jurídico nacional (Decreto nº 11.491/2023), que ampliam a cooperação internacional e aprimoram os mecanismos de investigação. Além disso, o trabalho aborda a importância das provas digitais como instrumento essencial na apuração da materialidade e autoria dos crimes virtuais, considerando suas particularidades em relação às provas tradicionais. Os resultados demonstram que, apesar dos significativos avanços legislativos, procedimentais e institucionais obtidos, ainda se faz necessária a implementação de novas medidas nas esferas legislativa e executiva, com o intuito de garantir maior eficiência, celeridade e eficácia às investigações conduzidas pelas instituições policiais.

Palavras-chave: Convenção de Budapeste. Dados. Prova digital.

DIGITAL CRIMINAL INVESTIGATION: THE CHALLENGES FACED BY THE JUDICIAL POLICE IN COMBATING CYBERCRIME

ABSTRACT

The present research aims to critically analyze the current structure of the Brazilian State in combating cybercrime, as well as to investigate the main challenges faced by judicial police authorities in the investigation of offenses committed in the digital environment. The study adopts the deductive method, based on the analysis of legislation, decrees, and international treaties related to the subject. It examines the normative and institutional advances that strengthen the performance of investigative authorities, with emphasis on Law No. 12.737/2012 (Carolina Dieckmann Law) and the incorporation of the Budapest Convention into the national legal system (Decree No. 11.491/2023), which expand international cooperation and improve investigative mechanisms. Furthermore, the paper addresses the importance of digital evidence as an essential instrument for determining the materiality and authorship of cybercrimes, considering its specific characteristics in comparison to traditional forms of evidence. The results demonstrate that, despite significant legislative, procedural, and institutional progress, it remains necessary to implement new measures within the legislative and executive spheres in order to ensure greater efficiency, speed, and effectiveness in investigations conducted by police institutions.

Keywords: Budapest Convention. Data. Digital evidence.

1 INTRODUÇÃO

A sociedade contemporânea é fortemente marcada pela expansão da internet e das tecnologias digitais, que são indispensáveis nas esferas sociais, profissionais e econômicas. Atualmente, bilhões de indivíduos em todo o mundo utilizam esses recursos para a realização de atividades diversas. Tais como, a comunicação em redes sociais, transações financeiras *online*, acesso a serviços de *streaming*, participação no comércio eletrônico e uso de plataformas de comunicação instantânea.

Todavia, o mesmo ambiente que promove facilidades e inovações também se revela propício à prática de delitos virtuais. O crescimento acelerado dos crimes cibernéticos evidencia um fenômeno global que desafia instituições policiais, tanto no Brasil quanto em outros países, exigindo a criação de novos mecanismos capazes de coibir tais práticas no meio digital.

No contexto brasileiro, embora tenham sido editadas legislações específicas visando um melhor enfrentamento dessas práticas, como a própria Lei nº 12.737/2012 (Lei Carolina Dieckmann), o ordenamento jurídico ainda demonstra limitações significativas para lidar com a complexidade e a dinamicidade próprias dos crimes digitais.

Diante deste contexto, a presente pesquisa justifica-se pela necessidade de analisar de forma crítica os desafios da investigação criminal no Brasil, e reflete sobre os limites legais da atuação policial e as dificuldades enfrentadas na identificação da autoria e preservação das provas. Busca-se também compreender por que a legislação e as práticas investigativas ainda não mostram-se totalmente eficazes no combate aos crimes cibernéticos os quais possíveis caminhos e ajustes possam ser propostos, de modo a fortalecer a persecução penal no que se refere aos crimes cometidos no meio digital.

Assim, ao contextualizar o estudo nos âmbitos nacional e internacional, evidencia-se que sua relevância está na contribuição para o debate científico e prático sobre a efetividade da investigação criminal digital, oferecendo subsídios tanto à comunidade acadêmica quanto à atuação dos operadores do direito e das instituições policiais.

2 DO CONCEITO, TIPIFICAÇÕES PENAIS EXISTENTES E EVOLUÇÃO LEGISLATIVA DOS CRIMES CIBERNÉTICOS

Segundo a definição de Queiroz (2024, p. 3), os crimes cibernéticos correspondem a infrações penais praticadas ou viabilizadas por meio da rede mundial de computadores, isto é, pela Internet. Tais condutas podem concretizar-se, tanto pelo uso abusivo desse recurso tecnológico quanto pela exploração inadequada de sistemas e aplicativos diversos.

Os delitos digitais, ainda segundo Queiroz (2024, p. 4), classificam-se em três categorias: 1) “crimes cibernéticos impróprios”, nos quais o computador funciona apenas como instrumento para a prática delituosa; 2) “crimes cibernéticos próprios”, que só podem ser cometidos mediante o uso de computadores ou dispositivos eletrônicos com acesso à Internet e 3)“crimes cibernéticos mistos”, em que a utilização da rede é requisito essencial para a execução da conduta criminosa, ainda que o bem jurídico lesado não seja diretamente o sistema informático.

Em uma análise dos crimes digitais presentes em nosso ordenamento jurídico brasileiro, é possível auferir que não há uma concentração dos tipos penais em uma única legislação, de forma que os crimes dessa espécie estão previstos tanto no Código Penal Brasileiro quanto em legislações esparsas, como o Estatuto da Criança e do Adolescente (Lei nº 8.069/90), Lei de Interceptações Telefônicas e de Dados (Lei nº 9.296/96), Lei de Software (Lei nº 9.609/98), entre outras. Desta forma, evidencia a diversidade de normas necessárias para abranger as mais variadas condutas criminosas cometidas no meio virtual.

No âmbito dos principais crimes tipificados no Código Penal, destacam-se os previstos nos arts. 154-A e 154-B, introduzidos pela Lei nº 12.737/2012 (Lei Carolina Dieckmann). Esses dispositivos estabelecem o delito de invasão de dispositivo informático, caracterizado pela prática de acessar sem autorização expressa do usuário, o sistema ou aparelho alheio com a finalidade de obter, adulterar ou destruir dados e informações, ou ainda de instalar vulnerabilidades com vistas à obtenção de vantagem ilícita.

Em relação ao Código Penal, destacam-se diversas condutas criminosas praticadas no ambiente digital. Entre elas, incluem-se os crimes contra a honra (arts. 138 a 141), que se estendem às ofensas veiculadas por meio de plataformas eletrônicas, o *cyberbullying* (art. 146-A), recentemente incorporado pela Lei nº 14.811/2024, que criminaliza atos de intimidação ou constrangimento reiterado contra terceiros no ambiente virtual.

Há também os crimes de perseguição digital ou “*stalking*” (art. 147-A) e estelionato por fraude eletrônica (art. 171, §2º-A), que abrange a obtenção de vantagem ilícita mediante artifícios digitais. Por fim, os crimes de falsidade ideológica e documental no meio eletrônico (arts. 298 e 299), que tipificam condutas fraudulentas envolvendo informações ou documentos digitais.

No âmbito da legislação esparsa, destacam-se diversos dispositivos relacionados a crimes cibernéticos. Entre eles, os arts. 241-A a 241-E do Estatuto da Criança e do Adolescente, que tratam de delitos envolvendo pornografia infantil. O art. 10 da Lei nº 9.296/1996, que tipifica a interceptação de comunicações de informática ou telemática sem

autorização judicial. Além do art. 184 da Lei de Direitos Autorais (Lei nº 9.610/1998), com aplicação subsidiária do Código Penal, que abrange a violação de direitos autorais, inclusive em ambiente digital, como ocorre em casos de pirataria, *downloads* ilegais e *streaming* não autorizado.

Com base nos tipos penais apresentados, é possível verificar um avanço significativo na tipificação de condutas criminosas no ambiente digital, garantindo a proteção de diversos bens jurídicos relevantes. No entanto, faz-se necessária uma atuação contínua e atualizada do Poder Legislativo, a fim de acompanhar novas condutas que possam lesar direitos ou causar prejuízos a indivíduos. Tal acompanhamento deve ser pautado por análises criteriosas de modo a prevenir eventuais excessos punitivos por parte do Estado.

2.1 A LEI Nº 12.737/2012 (LEI CAROLINA DIECKMANN)

A atriz brasileira Carolina Dieckmmann Worcman, renomada por diversos trabalhos realizados em novelas e filmes nacionais, foi vítima de uma ação criminosa no ano de 2011, quando hackers invadiram ilegalmente seu computador pessoal. Os criminosos tiveram acesso à 36 fotos íntimas da vítima, com isso, realizaram uma extorsão, e solicitaram uma quantia em dinheiro para que os arquivos digitais das fotos não fossem “vazados” na Internet, comprometendo a privacidade da vítima.

Em maio de 2012, a atriz teve suas fotos íntimas publicadas e divulgadas ilegalmente pela internet, diante da sua recusa em realizar o pagamento da quantia de dinheiro exigida pelos infratores. Na época causou uma grande repercussão e evidenciou uma lacuna legislativa no ordenamento jurídico brasileiro no que diz respeito ao combate e repressão aos crimes digitais. Em virtude da ausência de tipicidade da conduta dos criminosos naquela época, os suspeitos foram identificados e indiciados pelos delitos de furto, extorsão qualificada e difamação.

A partir desse caso, que teve ~~um~~ grande impacto nacional, surgiram amplas discussões sobre o tema no meio acadêmico e mídia. Houve uma mobilização do Congresso Nacional para aprovar um projeto de lei que alteraria o Código Penal Brasileiro, visando uma maior eficácia no combate aos crimes cibernéticos, sendo que, na data de 30 de novembro de 2012, houve o sancionamento da Lei nº 12.737. No entanto, a mesma legislação só entrou em vigor em abril de 2013, acrescendo os artigos 154-A e 154-B, além de alterarem redações nos artigos 266 e 298, todos do Código Penal.

A Lei nº 12.737/2012 passou a punir especificamente a invasão de dispositivos eletrônicos e outras condutas relacionadas a crimes cibernéticos. O artigo 154-A, tipificou o crime de invasão de dispositivo informático, que em sua redação originária previa expressamente a necessidade de comprovar a violação de forma indevida de um mecanismo de segurança para tipificar a conduta. Ademais, apresentava um conceito mais limitado e menos especificado do tipo penal, além de possuir uma pena de detenção de 3 (três) meses a 1 (um) ano e multa, o que tornava um tipo penal com pena considerada branda que se mostrou ineficaz em combater os indivíduos que praticavam esse tipo de crime cibernético.

Com a devida promulgação da Lei nº 12.737/2012, houve um marco significativo na repressão de condutas ilícitas praticadas no ambiente virtual, ao estabelecer uma previsão normativa específica para o delito de invasão de dispositivos eletrônicos ou informáticos. O artigo 154-A, em sua redação originária, tipificou o referido delito condicionado a necessidade de caracterização do delito à violação indevida de mecanismo de segurança. No entanto, o tipo penal apresentava um conceito limitado e pouco preciso, o que aliado a uma pena cominada relativamente branda, prevendo a detenção de 3 (três) meses a 1 (um) ano e multa, revelou-se insuficiente para atender às necessidades de repressão efetiva dessas condutas criminosas praticadas no meio digital.

Posteriormente, entrou em vigor a Lei nº 14.155/2021, que alterou substancialmente a redação original do artigo 154-A, suprimindo a exigência de comprovar violação de mecanismo de segurança, além de abranger a conduta de instalar vulnerabilidades em dispositivos informáticos com o intuito de obter vantagem ilícita. No tocante as sanções penais correspondentes, verificou-se uma ampliação punitiva, com o aumento da pena base para reclusão de 1 (um) a 4 (quatro) anos, cumulada com multa, além da majoração das hipóteses previstas nos §§ 2º e 3º do referido dispositivo legal.

Conforme exposto, é possível auferir que a promulgação da Lei Carolina Dieckmann representou um avanço crucial para a evolução legislativa no que tange ao combate aos crimes cibernéticos. Contudo, antes das alterações introduzidas pela Lei nº 14.155/2021, a norma foi alvo de críticas quanto à sua efetividade. Sobretudo em razão da cominação de penas consideradas brandas, que não se mostraram suficientes para desestimular eventuais novos infratores, especialmente em casos em que os danos ocasionados se revelavam expressivos. Deste modo, diante da pena mínima prevista, a necessidade de tramitação célere dos processos tornava-se imperativa, sob pena de ocorrência da prescrição e consequente impunidade, conforme apontam Bispo e Binto (2023, p. 10).

3 DAS PROVAS DIGITAIS E SUA VOLATIVIDADE

Antes de discorrer sobre o tema central deste trabalho,—— os desafios enfrentados pelas polícias judiciárias no transcorrer da investigação criminal digital —, é necessário compreender o principal elemento que viabiliza a responsabilização penal de indivíduos que cometem delitos nesse contexto: a prova digital.

De acordo como preceituam Saad, Rossi e Partata (2024, p.5), a prova digital, ou também chamada de *digital evidence*, pode ser compreendida como um conjunto de dados em um formato digital, estruturados no sistema binário, que são armazenados em meios eletrônicos ou transmitidos por redes de comunicação, sendo utilizados para representação de fatos ou ideias.

Nos ensinamentos de Badaró (2021, p.7), em seu artigo "*Os standards metodológicos de produção na prova digital e a importância da cadeia de custódia*", uma das principais diferenças percebidas entre as provas digitais e as provas comuns está em sua imaterialidade, uma vez que seus elementos ~~se~~ tratam-se de linguagens não naturais. Embora as informações contidas nos dados digitais possam ser compreendidas por quem as acessa, esses dados não apresentam uma materialidade imediatamente perceptível.

Ainda segundo os ensinamentos de Saad, Rossi e Partata (2024, p.5), em razão da imaterialidade, outra característica que as diferenciam das provas analógicas é a sua volatilidade. Tal particularidade ocorre porque os dados digitais são considerados frágeis e podem sofrer adulterações, de forma voluntária ou involuntária, bastando apenas uma simples modificação na sequência numérica ~~no~~ do código binário utilizado nas tecnologias computacionais.

Conforme se depreende de Kerr (2005, *apud* Saad, Rossi e Partata, 2024) e de Moura & Barbosa (2020, *apud* Saad, Rossi e Partata, 2024), as provas digitais podem ser coletadas por diversos meios, notadamente: a interceptação telemática de informações digitais; a extração de dados após a apreensão do dispositivo eletrônico; a requisição a terceiros, especialmente provedores de serviços de conexão e de aplicações na internet; a instalação sub-reptícia de *softwares* espiões para acesso ao dispositivo alvo, sendo esta última considerada ilícita, pois utiliza *malwares* para a invasão ilegal do equipamento informático.

No que se refere às possibilidades mencionadas anteriormente, é possível estabelecer uma relação direta com a atividade de polícia judiciária no exercício de suas atribuições investigativas. Quanto à interceptação telemática, destaca-se o disposto no art. 5º, inciso XII, da Constituição Federal de 1988, que garante o sigilo de comunicações de dados, admitindo sua quebra através de ordem judicial. No mesmo sentido, a Lei nº 9.296/96 regulamenta a

interceptação telefônica, e estende sua aplicação às comunicações de natureza informática e telemática. Tal dispositivo legal, em seu artigo 1º, *caput* e parágrafo único, versa sobre a possibilidade de realização dessas interceptações, desde que haja devidamente autorizada por ordem judicial, visando subsidiar investigações criminais e também instruir processos penais.

Com base na sustentação legal contido nos artigos 3º, inciso I, 4º e 5º da Lei nº 9.296/1996, extrai-se que o pedido formulado pela autoridade policial ao juízo deve ter fundamentação adequada, demonstrando a necessidade da medida para a apuração de infração penal e indicando, de forma clara, os meios que serão empregados. A norma também exige que a decisão judicial que autoriza a interceptação seja devidamente fundamentada, sob pena de nulidade, necessitando especificar a forma de execução da diligência. Ademais, tal diligência deve ser procedida em até quinze dias, sendo admitida a sua renovação por igual período, desde que se comprove efetivamente que o meio é indispensável para obtenção de prova fundamental e para o prosseguimento da investigação.

Outro meio que oportuniza a obtenção de provas digitais consiste na coleta de dados realizada após a apreensão do dispositivo eletrônico. A referida medida é viabilizada mediante expedição e o cumprimento de mandado de busca e apreensão, previsto legalmente no art. 240 do Código de Processo Penal. Tal dispositivo legal possibilita a apreensão de mídias físicas e dispositivos de armazenamento de dados, a fim de angariar elementos probatórios que auxiliem na verificação de materialidade e da autoria de delitos cometidos no ambiente virtual.

A manipulação dos dados digitais deve observar estritamente as etapas da cadeia de custódia, compreendida nos artigos 158-A a 158-F do Código de Processo Penal, dispositivos introduzidos pela Lei nº 13.964/2019, conhecida como “Pacote Anticrime”. O descumprimento injustificado dos procedimentos legalmente definidos pode ensejar no enfraquecimento da confiabilidade da perícia realizada e dos dados coletados, podendo comprometer a validade da prova digital obtida no âmbito da investigação criminal.

Outro método é a requisição a terceiros, usualmente os provedores de conexão e aplicações da internet. Como fonte importante que versa sobre o tema podemos citar a Lei nº 12.965/2014, conhecida como a Lei do Marco Civil da Internet. Esta lei estabeleceu princípios, garantias, direitos e deveres para o uso da rede global, além de diretrizes de atuação direcionadas aos entes federativos. O diploma normativo, embora não trate necessariamente de matéria penal, trouxe maior segurança jurídica ao disciplinar a atuação dos órgãos policiais quanto ao acesso de dados virtuais.

Em conformidade com o dispositivo mencionado, e mais especificamente em seu artigo 10, §3º, verifica-se que as autoridades administrativas, dentre as quais ~~se~~ incluem a polícia judiciária, possuem a prerrogativa legal de requisitar, sem a necessidade de autorização judicial, o acesso a dados meramente cadastrais, como a qualificação pessoal, filiação e endereço. No entanto, quando se trata de informações que envolvam de comunicações virtuais, registros de conexão, entre outros dados que revelem o conteúdo de interações eletrônicas, a obtenção dessas informações depende de prévia e expressa autorização judicial, em conformidade com o disposto na Lei nº 9.296/1996 e com o entendimento consolidado pelos tribunais superiores.

3.1 DAS COMPETÊNCIAS E DIFICULDADES ENFRENTADAS PELAS POLÍCIAS JUDICIÁRIAS NA INVESTIGAÇÃO DIGITAL

O poder de polícia é exercido pela Administração Pública por intermédio de seus agentes. Tal competência pode ser verificada legalmente na Constituição Federal de 1988, em seu artigo 144, incisos I e IV, que estabelece a regulamentação das instituições policiais, notadamente das polícias judiciárias. Embora não possuam caráter indispensável para o ajuizamento da ação penal, os elementos colhidos no inquérito policial são de suma importância para apuração de materialidade e autoria dos delitos, inclusive daqueles praticados no meio cibernético.

Conforme disciplina De Aguiar Corrêa (2009, p. 40), a polícia judiciária dispõe de competência específica para promover a apuração de fatos delituosos e a coleta preliminar dos elementos de prova que darão embasamento para a viabilidade de submeter determinado fato ao processo penal, constituindo-se, como instrumento que concretiza o direito punitivo do Estado. Dessa forma, a fase inicial do *jus puniendi* necessita ser conduzida por um órgão imparcial e externo ao subsequente processo penal, assegurando a indispensável distinção entre as funções de investigar, acusar e julgar. Tal separação é essencial para a efetiva proteção dos direitos fundamentais do cidadão, por meio da observância dos princípios do Devido Processo Legal e da Segurança Jurídica, pilares estruturantes do Estado Democrático de Direito.

Conforme afirma De Aguiar Corrêa (2009, p. 44), é notório que a polícia judiciária é a instituição que mais se aproxima da denominada verdade natural dos fatos, uma vez que é a primeira a ter contato direito com o delito após sua ocorrência. Isto posto, tal órgão dispõe de melhores condições de viabilizar a produção de provas que possam descrever com maior

fidelidade, o que realmente aconteceu em determinado fato que venha a ser objeto de investigação criminal.

Nos dizeres de Lima Filho e Santos (2025, p. 2), a investigação criminal tem seu papel no sistema jurídico frequentemente subestimado, preceituando que a doutrina e jurisprudência tradicionalmente conceituam o inquérito policial como um procedimento meramente preliminar, tese esta considerada superada pelos autores. A interpretação predominante sustenta que, em razão de sua natureza jurídica, o inquérito não assegura integralmente os direitos fundamentais do investigado, afastando-se, assim, a ideia de que se trate de um instrumento de proteção de garantias individuais. Todavia, cabe à Polícia Civil, como órgão auxiliar do Poder Judiciário, a atribuição de apurar infrações penais, sendo sua atuação mais ampla do que a mera condução e conclusão do inquérito policial.

Nos termos dos §§ 1º e 4º do artigo 144 da Constituição Federal de 1988, as polícias judiciárias se dividem entre a Polícia Federal e a Polícia Civil, cada uma com atribuições específicas e complementares. Quanto à Polícia Federal, esta exerce suas atribuições no âmbito da União, incumbindo-se da investigação de crimes que atentem contra bens, serviços ou interesses federais, bem como daqueles de repercussão nacional ou internacional que exijam repressão uniforme. Já a Polícia Civil, atua em esfera estadual, e possui~~ndo~~ competência para a apuração das infrações penais de natureza comum, exceto as de competência da União. Sua atuação, portanto, assume caráter subsidiário e cooperativo em relação à Polícia Federal.

No que se refere às competências da Polícia Federal no combate aos crimes digitais, além daquelas previstas constitucionalmente, pode-se destacar algumas legislações esparsas que delimitam a atuação do referido órgão federal. O Decreto nº 11.348/2023, em seu artigo 48, atribui à Diretoria de Combate a Crimes Cibernéticos a responsabilidade de investigar crimes cometidos no meio digital de alta complexidade tecnológica, especificamente aqueles que possam violar infraestruturas críticas, crimes de abuso sexual infanto-juvenil, bem como fraudes eletrônicas.

Ainda sobre as atribuições da Polícia Federal, a Lei nº 10.446/2002, que também regula sua atuação, prevê, em seu artigo 1º, inciso VII, a competência para apurar crimes cometidos por meio da rede mundial de computadores que disseminem conteúdo misógino, entendido como aquele que propaga ódio ou aversão às mulheres.

Quanto aos desafios enfrentados por estes órgãos no curso da investigação criminal digital, na percepção de Queiroz (2024, p. 5), existe uma necessidade legislativa de criação de uma norma específica e unificada que trate de maneira abrangente a questão dos crimes

cibernéticos. Além disso, observa-se que as penas atualmente previstas para tais delitos são brandas, o que compromete o efeito dissuasório esperado. Ainda segundo o autor, soma-se complexidade técnica das investigações, dificultadas pelo uso de redes criptografadas, endereços de IP compartilhados e mecanismos de anonimização, que tornam a identificação dos autores mais árdua e prolongam o tempo de resposta do sistema de justiça.

Acerca do mesmo tópico, De Sousa e Santos (2024, p. 7) e Pinheiro (2013, *apud* De Sousa e Santos, 2024, p. 7) preceituam que as polícias judiciárias enfrentam restrições técnicas, insuficiência de capacitação, escassez de recursos humanos especializados e um número reduzido de denúncias apresentadas pelas vítimas. Soma-se a esses fatores a fragilidade na coleta e na preservação das provas digitais, cuja volatilidade compromete a efetividade de sua utilização no processo penal, ampliando os desafios na persecução criminal.

Embora possamos observar que houve aprimoramentos legislativos, técnicos e informativos no que se diz respeito à repressão de crimes cometidos no âmbito virtual, persistem dificuldades significativas enfrentadas pelas polícias judiciárias na apuração desses delitos, especialmente na esfera das polícias civis, que dispõem de menor direcionamento orçamentário e estrutural em comparação com a Polícia Federal.

3.2 A CONVENÇÃO DE BUDAPESTE (DECRETO Nº 11.491/2023)

No cenário internacional, diante do crescente aumento de ocorrências delituosas praticadas no ambiente virtual e da necessidade global de aprimoramento e fortalecimento dos mecanismos de repressão e prevenção a tais crimes, o Conselho da Europa promoveu, no ano de 2001, na cidade de Budapeste, Hungria, a Convenção sobre o Crime Cibernético, também conhecida como Convenção de Budapeste. O referido tratado internacional foi considerado um marco ao enfrentamento dos crimes cibernéticos, uma vez que visou estabelecer uma harmonia legislativa sobre o tema entre os países signatários, padronização de procedimentos de investigação digital e a consolidação de uma cooperação global.

De acordo com o exposto por Fonseca e Gennarini (2022, p. 60), os objetivos do tratado mencionado não consistem em apenas harmonizar os dispositivos legais de direito material sobre o tema, mas também em estabelecer diretrizes de natureza processual no campo das investigações de crimes cometidos por meio de sistemas informáticos, assegurando a adequada preservação e rastreabilidade da cadeia de custódia das provas eletrônicas. Assim sendo, a Convenção de Budapeste recomenda que os Estados signatários adotem medidas legislativas e administrativas a fim de alterarem seus respectivos ordenamentos jurídicos

internos visando uma compatibilização com os padrões internacionais de combate ao crime cibernético.

Cumpre salientar que a Convenção sobre o Crime Cibernético, embora tenha sido firmada por vários países no ano de 2001, veio a ser recepcionada e ratificada pelo Brasil somente em 2022, após um exacerbado período de discussões acerca da adequação da legislação nacional aos padrões estabelecidos internacionalmente de enfrentamento aos delitos virtuais. A efetiva promulgação e inclusão da Convenção de Budapeste em nosso ordenamento jurídico brasileiro ocorreu em abril de 2023, através do Decreto nº 11.491, que deu vigência interna ao tratado, representando um momento significativo na consolidação da política criminal cibernética no país.

No que diz respeito à estrutura do tratado internacional, conforme preceituam Murata e Torres (2023, p. 13), a Convenção de Budapeste apresenta uma redação sistematicamente organizada em capítulos, visando uma clareza e efetividade de sua aplicação. O primeiro capítulo versa sobre conceitos e nomenclaturas da matéria, garantindo uma mútua compreensão entre os Estados subscritores. O segundo capítulo dispõe das medidas a serem implementadas no âmbito das jurisdições nacionais, subdividindo-se em três seções principais: Direito Penal, Direito Processual e Jurisdição. O terceiro capítulo, por sua vez, trata sobre a cooperação internacional, delimitando princípios orientadores e mecanismos de assistência jurídica internacional.

Por fim, o quarto e último capítulo da Convenção de Budapeste trata das disposições finais do tratado, consolidando e delimitando aspectos formais para a plena eficácia em âmbito internacional. Nesse capítulo, podemos destacar temas como a assinatura e entrada em vigor da Convenção, as regras referentes à adesão de novos Estados, a aplicação territorial de suas disposições e os efeitos jurídicos decorrentes de sua implementação. Essa parte do texto é de suma importância a fim de conferir segurança jurídica, estabilidade e previsibilidade quanto à aplicação das normas do pacto firmado.

Murata e Torres (2023, p. 14) advertem que é imprescindível que a incorporação de novas condutas tipificadas pela Convenção de Budapeste seja conferida com cautela e rigor técnico, a fim de evitar uma eventual sobreposição com os tipos penais já previstos em nosso ordenamento jurídico brasileiro, bem como resguardar a criação de um excesso punitivo do Estado incompatível com os princípios constitucionais. As autoras apontam que o processo de adequação normativa precisa seguir etapas como a adequada análise do bem jurídico tutelado, a formulação precisa das tipificações penais e a fixação de sanções proporcionais. A não observância desses passos, pode resultar na produção de uma norma penal ineficaz, suscetível

de gerar insegurança jurídica e de abrir espaço para interpretações arbitrárias no exercício do poder punitivo estatal.

No que se refere às implementações e recomendações legislativas de direito penal material introduzidas pela Convenção de Budapeste, destaca-se, inicialmente, crimes contra a confidencialidade, integridade e disponibilidade de dados e sistemas de computador, que propõe a criminalização de condutas como acesso ilegal a sistemas informáticos, interceptação ilícita de comunicações e violação de dados. Ademais, no que se refere aos crimes informáticos previstos nos artigos 7º e 8º do tratado, são sugeridas a tipificação da falsificação de dados informáticos, e a criminalização da fraude informática caracterizada pela obtenção de vantagem econômica ilícita mediante alteração de dados ou interferência em sistemas computacionais, resultando em prejuízo patrimonial a terceiros.

Por outro lado, o artigo 12 da Convenção levanta um debate relevante quanto à compatibilidade de suas disposições com o ordenamento jurídico brasileiro, ao prever a possibilidade de responsabilização penal de pessoas jurídicas pelos crimes tipificados em conformidade com o tratado. O dispositivo internacional estabelece que essa responsabilidade possa ser de natureza cível, penal ou administrativa, sem prejuízo da responsabilização individual das pessoas físicas envolvidas na prática delituosa. Ocorre que tal recomendação contraria a legislação brasileira, a qual adota a responsabilidade penal apenas das pessoas naturais, salvo exceções constitucionais expressas, como a questão de crimes ambientais.

A Convenção sobre o Crime Cibernético introduziu disposições de grande relevância para o fortalecimento do combate aos delitos virtuais, sobretudo por valorizar o princípio da cooperação internacional como ponto central de sua aplicação prática. Esses artifícios de colaboração entre os Estados signatários proporciona uma melhor atuação da Polícia Federal brasileira, especialmente em investigações que extrapolam os limites territoriais nacionais, envolvendo agentes, vítimas ou infraestruturas situadas em diferentes países. Em um contexto de globalização e interconectividade das comunicações e meios digitais, tal contribuição mútua torna-se indispensável no combate aos crimes digitais transfronteiriços, tendo em vista que exigem uma resposta rápida e coordenada entre as autoridades competentes.

Dentre as principais inovações trazidas pelo tratado internacional que auxiliam a atuação da polícia judiciária no curso das investigações criminais digitais, salienta-se o princípio geral da assistência mútua, previsto no artigo 25, que garante a troca de comunicações e dados entre os Estados signatários da Convenção de Budapeste. De igual modo, o artigo 26 introduz a questão da informação espontânea, a qual estabelece que um Estado transmita, por iniciativa própria, elementos de prova ou dados obtidos em suas

investigações internas a outro Estado-Parte, sempre que considerar que tais informações possam contribuir para o início ou o prosseguimento de apurações em curso.

No tocante às medidas cautelares, comumente essenciais à atuação das polícias judiciárias, o texto internacional define, em seu artigo 29, a viabilidade de um Estado signatário requisitar a outra autoridade competente a conservação expedita de dados armazenados em seu território, quando tais informações forem essenciais ao prosseguimento de investigações criminais. Contudo, tal requisição deve ser feita através de um pedido fundamentado, comunicando a natureza da investigação, as razões que justificam a urgência e a necessidade da medida cautelar, de modo a assegurar a preservação de elementos probatórios transfronteiriços antes que possam ser alterados ou destruídos.

Por fim, aponta-se a medida contida no artigo 31 da Convenção sobre o Crime Cibernético, possibilitando a solicitação de busca, acesso, apreensão, guarda ou revelação de dados armazenados em outros países, medida essa que se demonstra primordial para uma maior eficácia de inquéritos policiais envolvendo delitos cibernéticos cuja materialidade, autoria ou repercussão ultrapassem os limites territoriais do Brasil.

Em síntese, pode-se afirmar que a incorporação da Convenção de Budapeste representou um marco significativo no aprimoramento das investigações criminal digitais no Brasil, especificamente daquelas que envolvam partes ou matérias presentes em outros países. A adesão dos dispositivos da redação do tratado corrobora com o compromisso de fortalecer o poder de investigação das polícias judiciárias no enfrentamento de crimes cometidos no âmbito virtual, levando em consideração a necessidade do Estado brasileiro se adequar aos padrões estabelecidos internacionalmente que versam sobre o tema.

3.3 DAS MUDANÇAS E MELHORIAS SUGERIDAS

Quanto às perspectivas de aprimoramento e superação dos desafios enfrentados pelas polícias judiciárias no combate aos crimes cibernéticos, revela-se imprescindível a realização de uma reforma legislativa que consiga viabilizar o acesso célere e eficiente a dados digitais necessários para o curso de investigações. No entanto, tais mudanças devem observar limites constitucionais e garantias individuais dos cidadãos, assegurando que a obtenção dessas informações ocorra apenas diante de fundadas suspeitas e indícios concretos de materialidade e autoria delitiva. Diante de um ambiente digital que se torna cada vez mais complexo e tecnológico, surge a necessidade de uma modernização normativa a fim de garantir uma melhor efetividade na repressão de delitos dessa espécie.

Mostra-se igualmente fundamental, o investimento estatal na modernização da infraestrutura das delegacias de polícia judiciária, com a adoção de tecnologias atualizadas e avançadas que possibilitem o rastreamento mais eficiente de dispositivos e usuários envolvidos em crimes de natureza cibernética. Tal aprimoramento técnico deve vir acompanhado de medidas que promovam uma desburocratização dos procedimentos de requisição de dados telemáticos, garantindo uma melhor agilidade essencial para as investigações, sem desconsiderar preceitos constitucionais que asseguram a proteção da privacidade e da intimidade dos cidadãos.

Além dessas medidas, é primordial que o Estado invista na contratação e capacitação de novos policiais judiciários, especialmente nos órgãos em que há escassez de efetivo e notória defasagem de servidores, de modo a suprir as crescentes demandas decorrentes do aumento exponencial dos crimes cibernéticos. Esses agentes de segurança pública devem receber uma formação técnica especializada desde o curso de inicial de formação policial, assegurando que esses futuros profissionais estejam aptos a lidarem com a complexidade e a dinamicidade das investigações digitais. Tal providência não contribui apenas para o fortalecimento institucional das polícias judiciárias, mas também para assegurar uma maior eficácia na persecução penal e a proteção da sociedade frente às novas modalidades de criminalidade tecnológica.

Por fim, evidencia-se pertinente a implementação de políticas públicas e programas educacionais promovidos pelas polícias judiciárias, com o propósito de instruir e conscientizar a sociedade acerca dos riscos e das práticas delitivas no ambiente digital. As referidas ações devem ter como foco principal, sobretudo, os grupos com menor familiaridade com o uso da internet e das tecnologias da informação capacitando-os para reconhecer e evitar armadilhas virtuais, fraudes e demais crimes cibernéticos. Além disso, é essencial estimular a cultura da denúncia e da cooperação cidadã, uma vez que a prevenção se mostra mais eficaz do que a repressão, especialmente diante da elevada complexidade técnica e do esforço investigativo exigido para identificar e responsabilizar os autores dessas infrações no ciberespaço.

4 CONCLUSÃO

A presente pesquisa teve como objetivo principal realizar uma análise crítica dos principais desafios enfrentados pelas polícias judiciárias no combate aos crimes praticados no ambiente cibernético, considerando o contexto contemporâneo marcado pela globalização e pelos constantes avanços tecnológicos.

O desenvolvimento acelerado das inteligências artificiais, do tráfego massivo de dados e da circulação de informações digitais em alta velocidade tem proporcionado uma maior comodidade e conectividade aos usuários, em contrapartida, houve uma ampliação de possibilidades de utilização indevida desses recursos para a prática de ilícitos. Nesse contexto, o crescimento exponencial do número de usuários e dos serviços ofertados na internet torna o ciberespaço um terreno fértil para a ocorrência de delitos, impondo às instituições policiais o dever de apurar os fatos, identificar os responsáveis e promover a devida responsabilização penal, dentro dos limites legais e de suas atribuições previstas constitucionalmente.

No primeiro tópico, ao analisar os tipos penais atualmente previstos no ordenamento jurídico brasileiro referentes aos crimes digitais, observa-se um expressivo avanço legislativo na tipificação de condutas que não eram criminalizadas anteriormente. Diversas alterações e implementações foram introduzidas tanto no Código Penal quanto em legislações esparsas, adaptando o dispositivo legal às novas realidades tecnológicas. Nesse contexto, destaca-se a Lei nº 12.737/2012, ou Lei Carolina Dieckmann, que foi considerada um marco normativo no enfrentamento aos delitos cibernéticos, ao tipificar a invasão de dispositivos eletrônicos e outras condutas similares, por meio da inserção dos artigos 154-A e 154-B no Código Penal.

Quando discute-se sobre a apuração de crimes cibernéticos, torna-se imprescindível compreender o conceito e a natureza da prova digital, elemento central na atuação das polícias judiciárias, uma vez que é por meio dela que busca-se comprovar a materialidade e a autoria delitiva. As provas digitais apresentam características específicas que as diferenciam das provas tradicionais, especialmente quanto à sua imaterialidade e volatilidade, já que os dados digitais podem ser facilmente modificados, destruídos ou adulterados, exigindo técnicas específicas de coleta, preservação e análise, respeitando as etapas predefinidas da cadeia de custódia.

A distinção de competências entre as polícias judiciárias brasileiras, representadas pela Polícia Civil e pela Polícia Federal, é fundamental para compreender as atribuições específicas de cada instituição no enfrentamento dos crimes cibernéticos. Todavia, apesar da relevância institucional de ambas, é possível identificar desafios estruturais e operacionais que comprometem a eficiência das investigações digitais, tais como, limitações técnicas, falta de capacitação técnica, escassez de recursos humanos especializados e o baixo índice de denúncias apresentadas pelas vítimas, conforme já mencionado anteriormente nos dizeres de De Sousa e Santos (2024, p. 7) e Pinheiro (2013, *apud* De Sousa e Santos, 2024, p. 7).

A ratificação da Convenção sobre o Crime Cibernético, ou Convenção de Budapeste, representou um marco significativo para o aprimoramento da investigação criminal digital no

Brasil. Ao incorporar seus dispositivos ao ordenamento jurídico nacional, o país passou a integrar um sistema internacional de cooperação mútua entre os Estados signatários. Essa integração fortalece de forma expressiva a atuação das polícias judiciárias brasileiras, contribuindo no enfrentamento mais eficiente dos crimes cibernéticos e para a consolidação de um ambiente jurídico alinhado aos padrões internacionais de combate à criminalidade digital.

É evidente que há aperfeiçoamentos necessários na atuação das respeitáveis polícias judiciárias no enfrentamento ao crime cibernético, em decorrência de vários desafios expostos nesta pesquisa. Nesse sentido, mostra-se essencial a implementação de medidas estruturais e legislativas que possibilitem maior eficiência e celeridade nas investigações. Entre elas, destacam-se a modernização normativa, voltada à desburocratização da obtenção de dados digitais, o investimento estatal em infraestrutura tecnológica das delegacias e a contratação de novos policiais judiciários, de modo a suprir a carência de efetivo e garantir uma atuação mais técnica e qualificada.

Conforme todo o exposto, percebe-se que houve um desenvolvimento apreciável do país no combate aos crimes cibernéticos, especialmente ao longo do século XXI, por meio de aperfeiçoamentos legislativos, procedimentais e institucionais que fortalecem a atuação das polícias judiciárias e demais órgãos responsáveis pela persecução penal. Todavia, é imprescindível reconhecer que esse processo de aprimoramento deve ser contínuo e dinâmico, uma vez que a tecnologia evolui em ritmo acelerado, gerando novas formas de condutas delitivas que desafiam o sistema de justiça criminal.

Assim, cabe ao Estado, enquanto garantidor da segurança pública, do bem-estar social e da proteção dos direitos fundamentais, conforme preceitua a Constituição Federal, manter-se vigilante na criação de políticas, investimentos e atualizações normativas, assegurando que a estrutura estatal acompanhe as transformações tecnológicas e continue apta a proteger a sociedade frente aos riscos do ambiente digital.

REFERÊNCIAS

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil de 1988. Brasília: Presidência da República, 2025. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/ConstituicaoCompilado.htm. Acesso em: 01 out. 2025.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm. Acesso em: 01 out. 2025.

BRASIL. Decreto-Lei nº 3.689, de 3 de outubro de 1941. Código de Processo Penal. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 01 out. 2025.

BRASIL. Decreto nº 11.491, de 10 de outubro de 2023. Promulga a Convenção sobre o Crime Cibernético. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11491.htm. Acesso em: 01 out. 2025.

BRASIL. Lei nº 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 01 out. 2025.

BRASIL. Lei nº 9.296, de 24 de julho de 1996. Regula a interceptação de comunicações telefônicas e de outras formas de comunicação. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em: 01 out. 2025.

BRASIL. Lei nº 9.610, de 19 de fevereiro de 1998. Altera, atualiza e consolida a legislação sobre direitos autorais. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9610.htm. Acesso em: 01 out. 2025.

BRASIL. Lei nº 10.446, de 8 de maio de 2002. Dispõe sobre a atuação da Polícia Federal em infrações penais que envolvam interesse da União. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10446.htm. Acesso em: 01 out. 2025.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos (Lei Carolina Dieckmann). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 01 out. 2025.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (Marco Civil da Internet). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 01 out. 2025.

QUEIROZ, Liv Ferreira Augusto Severo. Os crimes cibernéticos no ordenamento jurídico brasileiro: investigação criminal e desafios. *Revista do CNMP*, n. 12, p. 417-448, 2024.

DA SILVA BISPO, Adrielle; BINTO, Emanuel Vieira. Crimes Cibernéticos: da ineficácia da Lei Carolina Dieckmann na prática de crimes virtuais. *Revista Ibero-Americana de Humanidades, Ciências e Educação*, v. 9, n. 11, p. 354-369, 2023.

SAAD, Marta; ROSSI, Helena Costa; PARTATA, Pedro Henrique. A obtenção das provas digitais no processo penal demanda uma disciplina jurídica própria? Uma análise do conceito,

das características e das peculiaridades das provas digitais. *Revista Brasileira de Direito Processual Penal*, v. 10, n. 3, p. e1071, 2024.

BADARÓ, Gustavo Henrique Righi Ivahy. Os standards metodológicos de produção na prova digital e a importância da cadeia de custódia. *Boletim IBCCRIM*, v. 29, n. 343, p. 7-9, 2021.

DE AGUIAR CORRÊA, Vanessa Pitrez. O papel da polícia judiciária no Estado Democrático de Direito. *Revista do Tribunal Regional Federal da 1ª Região*, v. 21, n. 1, 2009.

LIMA FILHO, Eujécio Coutrim; DOS SANTOS, Carlos Magnu Ferreira. A investigação criminal como instrumento público de supremacia da persecução criminal: um estudo crítico-analítico acerca da essencialidade do inquérito policial. *Avante: Revista Acadêmica da Polícia de Minas Gerais*, v. 1, n. 8, 2025.

DE SOUSA, Carlos Muryllo Rodrigues; SANTOS, Guilherme Augusto Martins. Crimes cibernéticos e os desafios jurídicos na era digital: análise legislativa, doutrinária e jurisprudencial. *Revista JRG de Estudos Acadêmicos*, v. 7, n. 15, p. e151662-e151662, 2024.

FONSECA, Marcos De Lucca; GENNARINI, Juliana Caramigo. A adesão do Brasil à Convenção de Budapeste e os impactos para a produção de provas digitais. *Direito Penal e Processo Penal*, v. 4, n. 1, p. 55-70, 2022.

MURATA, Ana Maria Lumi Kamimura; TORRES, Me Paula Ritzmann. A Convenção de Budapeste sobre os crimes cibernéticos foi promulgada, e agora? *Boletim IBCCRIM*, v. 31, n. 368, 2023.