CENTRO UNIVERSITÁRIO DE MACEIÓ
CURSO DE DIREITO
GRADUAÇÃO EM DIREITO

CLEMILDA MARIA DE OLIVEIRA CAVALCANTE JATOBÁ

OS DESAFIOS ENFRENTADOS NA INVESTIGAÇÃO DOS CRIMES CIBERNÉTICOS

MACEIÓ
2025

CLEMILDA MARIA DE OLIVEIRA CAVALCANTE JATOBÁ

OS DESAFIOS ENFRENTADOS NA INVESTIGAÇÃO DOS CRIMES CIBERNÉTICOS

Monografia de conclusão de curso, apresentada à Coordenação do Curso de Direito como requisito parcial, para obtenção do grau de Bacharel em Direito.

Orientador: Prof. Bruno Barbosa Sarmento

Assinatura do Orientador

MACEIÓ
2025

J39d

Jatobá, Clemilda Maria de Oliveira Cavalcante
Os desafios enfrentados na investigação dos crimes cibernéticos / Clemilda Maria de Oliveira Cavalcante Jatobá ; orientação [de] Bruno Barbosa Sarmento. – Maceió, 2025.
55 f. : il.

Trabalho de Conclusão de Curso (Graduação em Direito) - AFYA Centro Universitário UNIMA | Afya Maceió, 2025.

Inclui Bibliografias.

1. Crimes cibernéticos. 2. Estelionato digital. 3. Investigação Criminal. I. Sarmento, Bruno Barbosa. (orient.). II. Centro Universitário de Maceió. III. Título.

CDU: 34

Catalogação na fonte: Biblioteca do Centro Universitário de Maceió, Unima | Afya

Bibliotecária responsável: Adriele da Silva Lima CRB-4/1898

Ao meu pai, Hélio, cuja força e dedicação me mostraram que a determinação constrói caminhos. À minha família, que com amor e apoio incondicional, sustentou cada passo desta caminhada. Aos meus amigos e amigas, que estiveram ao meu lado nos momentos de desafio e celebração. Recebam meu mais profundo agradecimento.

RESUMO

O presente trabalho visa analisar os desafios enfrentados na investigação de crimes cibernéticos, com ênfase no estelionato digital, considerando o cenário atual de acelerada digitalização e intensa inclusão tecnológica. A popularização da internet e dos dispositivos móveis trouxe inúmeros benefícios à sociedade, mas também ampliou exponencialmente as vulnerabilidades exploradas por criminosos no ambiente virtual. Nesse contexto, a problematização do estudo concentra-se nas dificuldades jurídicas, técnicas e institucionais para identificar e responsabilizar autores de delitos digitais, tendo em vista que a natureza transnacional, a volatilidade das provas e o uso de tecnologias de anonimização e criptografia impõem barreiras significativas à persecução penal. Além disso, a investigação exige integração multissetorial entre órgãos policiais, Ministério Público, Judiciário, autoridades reguladoras, empresas privadas e especialistas técnicos, o que nem sempre ocorre de forma coordenada, gerando morosidade e ineficiência. A ausência de estruturas especializadas em muitas regiões, aliada à indefinição de competências jurisdicionais e à resistência de alguns provedores em fornecer dados, contribui para a sensação de impunidade. Por outro lado, experiências de cooperação nacional e internacional, forças-tarefas e parcerias público-privadas indicam caminhos promissores para superar os entraves investigativos. Assim, este estudo busca compreender como a modernização legislativa, o fortalecimento institucional e a adoção de tecnologias avançadas podem contribuir para um modelo investigativo mais eficaz, garantindo a proteção da sociedade e o respeito aos direitos fundamentais na era digital.

Palavras-chave: Crimes cibernéticos. Estelionato digital. Investigação Criminal.

SUMÁRIO

INTRODUÇÃO 6

CAPÍTULO I OS DESAFIOS NA INVESTIGAÇÃO DOS CRIMES CIBERNÉTICOS 8

1.1 Contextualização Histórica e Tecnológica 8
1.2 Conceito de Crimes Cibernéticos 9
1.3 Histórico dos Crimes Cibernéticos 10
1.4 Desafios na Investigação dos Crimes Cibernéticos 12
1.4.1 Inovações e Tendências Futuras 12
1.5 O crime de Estelionato na Esfera Digital 13
1.6 Considerações Finais do Capítulo 13

CAPÍTULO II CRIMES CIBERNÉTICOS: INVESTIGAÇÃO E DIFICULDADES ENFRENTADA 15

2.1 Expansão da Cibercriminalidade 15
2.2 Autoridades Envolvidas no Combate aos Crimes Cibernéticos 17
2.3 Procedimentos na Investigação de Crimes Cibernéticos 21
2.4 Cooperação Investigativa e Atuação Multisetorial 27
2.5 Colaboração Técnica nas Investigações 31
2.6 Obstáculos à Persecução Cibernética 33
2.7 Considerações Finais 37

CAPÍTULO III CASOS PRÁTICOS E PRECEDENTES 38

3.1 Casos Relevantes de Estelionato Cibernético 38
3.2 Análise de Julgados e o seu Impacto na Investigação dos Crimes Cibernéticos 41

CONCLUSÃO 44

REFERÊNCIAS 46

INTRODUÇÃO

Nas últimas décadas, a transformação digital, impulsionada pela popularização da internet e pelo avanço das tecnologias de informação e comunicação, remodelou de forma profunda as interações sociais, econômicas e institucionais. O espaço virtual, antes restrito a fins acadêmicos e militares, tornou-se um ambiente indispensável para atividades cotidianas como comércio, educação, entretenimento e prestação de serviços. No Brasil, a rápida expansão da conectividade, especialmente a partir da popularização dos dispositivos móveis, permitiu que milhões de pessoas tivessem acesso à rede mundial, ampliando as possibilidades de interação e negócios. Contudo, ao lado das oportunidades, surgiram vulnerabilidades significativas, criando um cenário propício para o aumento exponencial da criminalidade no ambiente digital.

Nesse contexto, os crimes cibernéticos consolidaram-se como uma das maiores ameaças à segurança pública contemporânea. Delitos como invasão de sistemas, roubo de dados, disseminação de malwares e, em especial, o estelionato digital, ganharam espaço e sofisticação, explorando falhas técnicas, jurídicas e comportamentais. Entre as modalidades mais recorrentes estão fraudes financeiras, clonagem de contas em aplicativos de mensagens e golpes em plataformas de comércio eletrônico, que causam prejuízos bilionários e afetam milhões de brasileiros anualmente. A característica transnacional da internet, associada à volatilidade das provas digitais e ao uso de tecnologias de anonimização e criptografia, impõe barreiras significativas à atuação das autoridades, tornando a investigação mais complexa e demorada.

O estelionato digital, foco deste estudo, é tipificado pelo artigo 171, §2º, do Código Penal, com pena agravada para práticas cometidas mediante fraude eletrônica. Sua crescente incidência evidencia a capacidade de adaptação dos criminosos às novas tecnologias, bem como a dificuldade do sistema de justiça penal em responder de forma célere e eficaz. A execução desses delitos é favorecida por fatores como a fragilidade de sistemas de segurança, a falta de conscientização dos usuários e a facilidade de acesso a ferramentas digitais que permitem mascarar a identidade dos autores.

Este trabalho tem como objetivo geral analisar os principais desafios enfrentados na investigação de crimes cibernéticos, com ênfase no estelionato digital. A justificativa para essa análise reside na relevância social, jurídica e econômica da temática, considerando que, em um mundo cada vez mais conectado, a proteção do ambiente virtual tornou-se elemento essencial para a preservação da confiança nas interações digitais. A ineficiência na apuração desses

crimes não apenas alimenta a sensação de impunidade, mas também incentiva a continuidade das práticas ilícitas, comprometendo a segurança de cidadãos, empresas e instituições públicas.

No desenvolvimento do estudo, serão abordados aspectos como a atuação das autoridades competentes — Polícia Civil, Polícia Federal, Ministério Público, órgãos reguladores e entidades privadas —, os procedimentos técnicos e legais adotados, e as estratégias de cooperação nacional e internacional. Além disso, serão discutidos obstáculos recorrentes, como a ausência de unidades especializadas em determinadas regiões, a morosidade processual, a dificuldade de acesso a dados mantidos por provedores e a insuficiência de ferramentas tecnológicas para quebra de criptografia e análise forense avançada.

A pesquisa também analisará iniciativas promissoras, como forças-tarefas, grupos interinstitucionais e parcerias público-privadas, que demonstram potencial para mitigar entraves investigativos e aumentar a eficácia das apurações. Nesse sentido, pretende-se contribuir para o debate acerca da necessidade de modernização legislativa, fortalecimento institucional e adoção de tecnologias de ponta, como inteligência artificial e blockchain, no combate à criminalidade digital.

Dessa forma, este trabalho busca compreender, de forma ampla e crítica, os fatores que dificultam a persecução penal dos crimes cibernéticos e propor reflexões sobre medidas que possam aprimorar a atuação estatal frente a esse fenômeno. Ao explorar a intersecção entre tecnologia, direito e segurança pública, pretende-se oferecer subsídios para a construção de políticas e práticas mais eficazes, capazes de garantir a proteção dos direitos fundamentais e a segurança jurídica no ambiente digital.

CAPÍTULO I
OS DESAFIOS NA INVESTIGAÇÃO DOS CRIMES CIBERNÉTICOS

1.1 Contextualização Histórica e Tecnológica

A globalização, intensificada sobretudo após o fim da Guerra Fria, provocou profundas mudanças nas dinâmicas econômicas, políticas e culturais ao redor do mundo. Entre os fatores centrais desse processo está o avanço das tecnologias de informação e comunicação (TICs), cuja principal expressão é a internet. Criada inicialmente nos Estados Unidos, ainda na década de 1970, com o projeto ARPANET e o protocolo TCP/IP, a rede tinha fins militares e acadêmicos. No entanto, a partir da década de 1990, com o surgimento da *World Wide Web*, passou a integrar o cotidiano de milhões de pessoas e empresas, tornando-se uma infraestrutura global essencial para múltiplas atividades humanas, como comércio, educação, saúde e entretenimento (CASTELLS, 2018).

A internet não apenas ampliou a circulação de informações em escala global, mas também transformou profundamente as formas de produção, trabalho e sociabilidade. O espaço digital passou a abrigar atividades econômicas inteiras, como o *e-commerce*, as *fintechs* e as plataformas de *streaming*, além de redes sociais e ambientes colaborativos que moldam relações interpessoais e profissionais. Essa reconfiguração das estruturas sociais e produtivas tornou o ambiente virtual não apenas um meio de interação, mas também um novo território onde ocorrem disputas de poder, estratégias de marketing, influências políticas e, inevitavelmente, ações criminosas.

No contexto brasileiro, a expansão da internet se deu de maneira acelerada nas duas primeiras décadas do século XXI, sobretudo devido à popularização dos dispositivos móveis. A democratização do acesso, favorecida por políticas públicas, pela redução do custo dos equipamentos e pela ampliação das redes de telefonia, permitiu que milhões de pessoas se conectassem à rede mundial. Segundo dados do IBGE (2023), mais de 90% dos domicílios brasileiros possuem acesso à internet, o que evidencia o avanço da digitalização em diferentes regiões do país, inclusive nas áreas menos favorecidas.

Essa conectividade crescente trouxe inúmeros benefícios para a sociedade brasileira, como o aumento da inclusão digital, o acesso a serviços bancários online, a realização de consultas médicas remotas, a participação em cursos de educação a distância e a facilitação de processos burocráticos. Ao mesmo tempo, porém, criou vulnerabilidades, especialmente no campo da segurança digital. Castells (2018) destaca que as redes digitais reestruturaram a

sociabilidade, enquanto Bauman (1999) aponta a insegurança decorrente da fluidez das relações virtuais, configurando um cenário propício ao estudo dos desafios investigativos.

Esses crimes, que vão desde fraudes e invasões de sistemas até o sequestro de dados e a disseminação de fake *news*, representam um desafio crescente para autoridades, empresas e cidadãos. O anonimato e a velocidade do ambiente digital dificultam a identificação dos autores e a responsabilização penal, o que exige respostas complexas do sistema de justiça criminal.

Além disso, a evolução constante das tecnologias obriga os órgãos públicos e instituições a se atualizarem de forma permanente. As práticas criminosas cibernéticas não são estáticas: elas acompanham os avanços da tecnologia, explorando brechas em sistemas, aplicativos, redes sociais e mecanismos de segurança. Por isso, a investigação desse tipo de crime demanda conhecimento técnico especializado, cooperação internacional e normativas atualizadas, temas que serão aprofundados nos capítulos seguintes.

1.2 Conceito de Crimes Cibernéticos

Crimes cibernéticos são definidos como condutas ilícitas executadas por meio de tecnologias digitais, direcionadas a sistemas, redes e dados (KASPERSKY, 2025). No Brasil, a Lei nº 12.737/2012 (Lei Carolina Dieckmann) tipifica a invasão de dispositivos informáticos, enquanto o Código Penal aborda fraudes e ameaças virtuais (BRASIL, 2012; MPU, 2021). Roque (2005, apud URI Erechim, 2024) conceitua tais delitos como ações em que o computador atua como instrumento ou alvo, complementado pela INTERPOL (2015), que inclui pirataria, pornografia infantil e espionagem. Rosa (2002) amplia essa definição ao envolver dispositivos conectados, como smartphones, caracterizando infrações digitais. A natureza evolutiva desses crimes, influenciada por avanços tecnológicos, demanda atualizações contínuas na legislação e nas estratégias investigativas (AKAMAI, 2005; JUSBRASIL, 2023), servindo como base para análises futuras neste trabalho.

Quadro: Definições de Crimes Cibernéticos

Autor/Entidade	**Definição de Crime Cibernético**	**Ano**
Roque (apud URI)	Computador como instrumento ou objeto	2005

INTERPOL	Fraude à segurança de sistemas e redes	2015
Rosa	Conduta ilegal via dispositivos conectados	2002
Lei nº 12.737/2012	Invasão do dispositivo informático	2012
Kaspersky	Atividades ilegais em sistemas, redes e dados	2025

Fonte: Elaborado pela autora (2025)

O quadro apresentado oferece uma visão panorâmica das definições de crimes cibernéticos, destacando a diversidade de enfoques que vão desde a perspectiva técnica, como a de Roque (2005), até a abordagem legal da Lei nº 12.737/2012. A inclusão de entidades internacionais, como a INTERPOL (2015) e a Kaspersky (2025), reflete a complexidade global, enquanto a evolução temporal das definições sublinha a adaptação às tecnologias emergentes.

A análise do quadro revela a necessidade de uma integração conceitual, pois lacunas entre definições técnicas (ex.: ROSA, 2002) e normativas (ex.: Lei nº 12.737/2012) impactam a eficácia das investigações. Essa disparidade evidencia a importância de harmonizar os enfoques nacionais e internacionais, especialmente no que tange à legislação, às práticas de investigação e à cooperação internacional, aspectos que serão aprofundados nos capítulos subsequentes.

1.3 Histórico dos Crimes Cibernéticos

Os primórdios dos crimes cibernéticos envolveram ações básicas, como a disseminação de vírus. O caso do vírus "*I LOVE YOU*", em 5 de maio de 2000, infectou mais de 50 milhões de computadores, exigindo intervenções de entidades como o Parlamento Britânico e a CIA (GONÇALVES, 2001; SMITH, 2000). Em 2000, o ataque "*Mafiaboy*", perpetrado por um adolescente contra sites como eBay e Amazon, expôs vulnerabilidades da rede, marcando um

alerta global (JOHNSON, 2001).

Com o avanço tecnológico, os delitos escalaram para fraudes financeiras, roubo de identidade e ataques a infraestruturas críticas (CAZAROTI, PINHEIRO, 202; CÂMARA DOS DEPUTADOS, 2017). No Brasil, o Anuário de Segurança Pública (2023) estima prejuízos de R$ 186 bilhões entre julho de 2023 e julho de 2024, com 80 milhões de vítimas, enquanto a Trend Micro (2023) reporta 1,2 milhão de ataques a dispositivos móveis em 2023, um aumento de 10%. Para ilustrar a correlação entre a expansão da internet e o crescimento dos crimes cibernéticos, o gráfico a seguir apresenta estimativas baseadas em dados disponíveis:

Gráfico 1: Evolução da Penetração da Internet e Crimes Cibernéticos no Brasil (2018-2024)

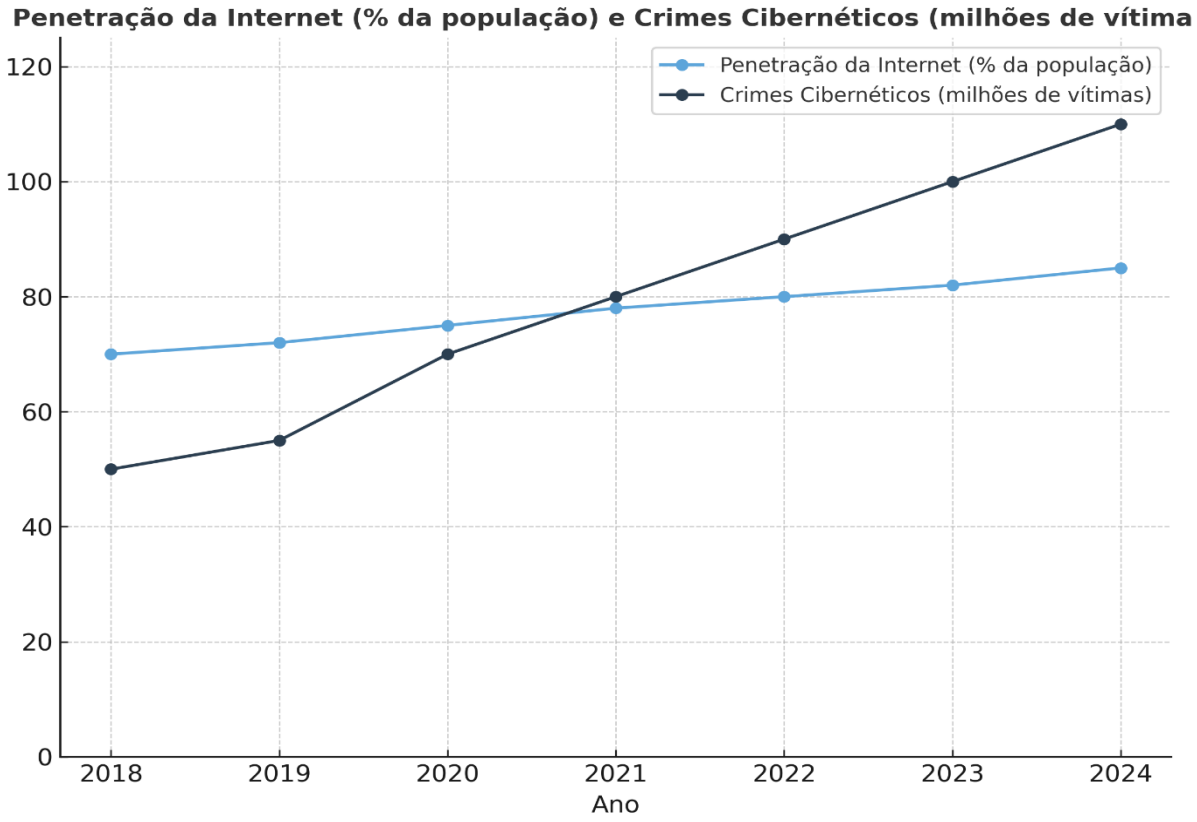


Gráfico elaborado pela autora (2025), baseado em estimativas de IBGE (2023), Anuário de Segurança Pública (2023), Trend Micro (2023), e Instituto Igarapé (citado em fontes diversas).

O gráfico ilustra a relação entre o aumento da penetração da internet e o crescimento dos crimes cibernéticos no Brasil entre 2018 e 2024. A linha azul claro, representando a porcentagem da população com acesso à internet, mostra um crescimento constante, atingindo 85% em 2024, conforme projeções baseadas em dados do IBGE (2023). Paralelamente, a linha

azul escuro, que indica o número estimado de vítimas de crimes cibernéticos (em milhões), reflete um aumento significativo, passando de 50 milhões em 2018 para 110 milhões em 2024. Essa tendência sugere uma correlação direta, reforçando a hipótese de que a digitalização amplifica a exposição a riscos cibernéticos, um ponto central para as análises dos capítulos seguintes.

As estimativas apresentadas no gráfico, embora baseadas em fontes confiáveis como o Anuário de Segurança Pública e a Trend Micro, possuem limitações devido à ausência de séries completas e oficiais para todos os anos. Os valores para 2024 são projeções, refletindo a continuidade das tendências observadas. Essa análise reforça a urgência na formulação de políticas públicas robustas e na modernização dos instrumentos legais e tecnológicos, visando mitigar o crescimento exponencial dos delitos cibernéticos.

1.4 Desafios na Investigaçãoo dos Crimes Cibernéticos

A investigação de crimes cibernéticos enfrenta obstáculos estruturais e técnicos. Greco (2021) e Nucci (2022) destacam a falta de capacitação dos agentes e a ausência de infraestrutura adequada como barreiras centrais. O anonimato, a volatilidade das informações e a atuação transnacional dos criminosos, aliados ao uso de criptografia e inteligência artificial, dificultam a rastreabilidade (CORREA JÚNIOR, 2024). A demora em decisões judiciais para quebras de sigilo e a dependência de cooperação internacional agravam o cenário (SALOMÉ & PAULA, 2023).

Diferentemente das apurações tradicionais, baseadas em evidências físicas, as investigações digitais requerem análise de dados em dispositivos, servidores e nuvens, demandando expertise em segurança da informação. A colaboração interdisciplinar, envolvendo policiais, peritos forenses e especialistas em direito digital, é indispensável (FOCO PUBLICAÇÕES, 2024). Ferramentas como análise forense digital e softwares de decodificação, embora promissoras, enfrentam limitações devido à falta de padronização e recursos, apontando a necessidade de investimentos em treinamento e tecnologia (REVISTA FT, 2025).

1.4.1 Inovações e Tendências Futuras

O avanço tecnológico também oferece oportunidades investigativas. O uso de inteligência artificial por autoridades para identificar padrões de comportamento criminoso e a implementação de blockchain para rastreamento de transações ilícitas emergem como

tendências (SILVA & ALMEIDA, 2024). Contudo, a adoção efetiva dessas inovações exige não apenas investimentos, mas também a formulação de políticas públicas coordenadas, atualização constante dos operadores do direito e fortalecimento da cooperação internacional, sob pena de tornar ineficaz o combate à criminalidade digital

1.5 O Crime de Estelionato na Esfera Digital

O estelionato digital, foco deste estudo, consiste na obtenção de vantagem ilícita por meio de fraudes virtuais, tipificado no artigo 171, §2º, do Código Penal, alterado pela Lei nº 14.155/2021, com pena de quatro a oito anos de reclusão (BRASIL, 1940; PLANALTO, 2021). Modalidades como clonagem de contas no WhatsApp, em que criminosos solicitam transferências sob falsos pretextos, e fraudes em compras online, com entrega de produtos inexistentes, exemplificam sua prevalência (TJDFT, 2022). Dados do Fórum Brasileiro de Segurança Pública (2025) indicam um aumento de 15% nos casos entre 2023 e 2024, com prejuízos estimados em R$ 50 bilhões anuais.

A caracterização legal exige a comprovação de dolo, artifício e prejuízo (Cunha, 2024), sendo os desafios investigativos agravados pela anonimização de criminosos e o uso de servidores internacionais. Jurisprudências recentes, como o caso julgado pelo Tribunal de Justiça do Distrito Federal (TJDFT, 2023), destacam a dificuldade de obtenção de provas em tempo hábil, sugerindo a necessidade de legislações mais ágeis e cooperação com provedores, tópicos a serem aprofundados nos próximos capítulos (OLIVEIRA, SILVA & ALMEIDA, 2025; JUSBRASIL, 2024).

1.6 Considerações Finais do Capítulo

Diante do exposto, percebe-se que os crimes cibernéticos representam um dos maiores desafios da contemporaneidade, tanto pelo seu caráter transnacional quanto pela constante evolução tecnológica que os alimenta. A contextualização histórica demonstrou como a digitalização da sociedade, embora traga inúmeros benefícios, também amplia exponencialmente os riscos relacionados à segurança virtual. A análise conceitual revelou que ainda há divergências e lacunas nas definições de crime cibernético, tanto no âmbito técnico quanto jurídico, o que impacta diretamente a eficácia dos processos investigativos.

O panorama histórico e estatístico evidencia que, à medida que o acesso à internet cresce, os crimes digitais se tornam mais sofisticados e frequentes, exigindo uma atuação igualmente qualificada por parte das autoridades competentes. As dificuldades enfrentadas nas

investigações — como o anonimato dos autores, a volatilidade das provas e os entraves da cooperação internacional — reforçam a urgência de modernização das práticas e das estruturas de combate.

Por fim, ao destacar o estelionato digital como objeto específico deste estudo, observa se que este tipo penal reflete com clareza os desafios da era digital, tanto na sua prática criminosa quanto nas barreiras jurídicas e operacionais para sua repressão. Assim, os temas aqui abordados não apenas introduzem a problemática dos crimes cibernéticos, como também fundamentam a necessidade de aprofundamento nas estratégias jurídicas, tecnológicas e institucionais, que serão analisadas nos capítulos subsequentes.

CAPÍTULO II
CRIMES CIBERNÉTICOS: INVESTIGAÇÃO E DIFICULDADES ENFRENTADAS

2.1 Expansão da Cibercriminalidade

O aumento expressivo dos crimes cibernéticos no Brasil configura um cenário preocupante e desafiador para as autoridades tradicionais. Nos últimos anos, o país tem vivenciado uma verdadeira epidemia dessas infrações, impulsionada pelo avanço tecnológico e pela crescente inclusão digital, que ampliam as oportunidades para a prática de delitos no ambiente virtual. Em 2023, 81% da população brasileira tinha acesso à internet, segundo o IBGE (2023), o que ampliou o alcance de plataformas digitais e, consequentemente, as vulnerabilidades exploradas por criminosos.

Dados alarmantes evidenciam a gravidade da situação: somente no primeiro semestre de 2022, o Brasil sofreu cerca de 31,5 bilhões de tentativas de ataques cibernéticos, representando um aumento de 94% em relação ao ano anterior (NORTON, 2022). Em 2024, foram registrados cerca de 5 milhões de fraudes digitais, um crescimento de 45% em relação a 2023 (FEBRABAN, 2024). Além disso, o Anuário Brasileiro de Segurança Pública de 2023 apontou um aumento de 65,2% nos registros de vítimas de golpes digitais em 2022 (FBSP, 2023).

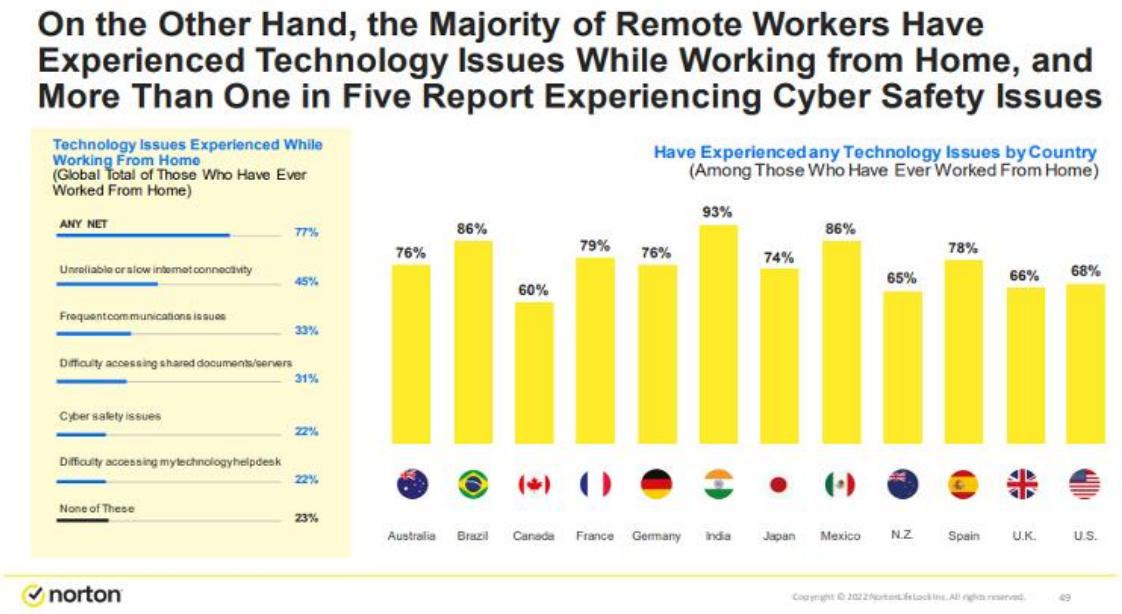
Tabela 1: Crescimento de Vítimas de Golpes Digitais no Brasil (2021-2022)

Ano	Vítimas de Golpes Digitais	Variação (%)
2021	1.200.000	-
2022	1.982.400	+65,2%

Fonte: Anuário Brasileiro de Segurança Pública (2023)

A Tabela 1 ilustra o crescimento alarmante no número de vítimas de golpes digitais no Brasil, passando de 1,2 milhão em 2021 para aproximadamente 1,98 milhão em 2022, uma variação de 65,2%. Esse aumento reflete a intensificação de práticas como estelionato virtual, phishing e roubo de identidade, impulsionadas pela maior dependência de plataformas digitais, especialmente durante a pandemia. Esses dados destacam a urgência de fortalecer as capacidades investigativas e preventivas das autoridades para mitigar o impacto social e econômico desses crimes.

Gráfico 1 – Trabalhadores remotos que relataram problemas tecnológicos ao trabalhar de casa, por país



Fonte: NortonLifeLock (2022)

O Gráfico 1 evidencia os desafios enfrentados por trabalhadores remotos brasileiros em relação à segurança digital. Segundo dados do Norton Cyber Security Insights Report (2022), o Brasil aparece entre os países com maior incidência de problemas tecnológicos durante o trabalho remoto, com 86% dos entrevistados relatando algum tipo de dificuldade — número significativamente acima da média global (77%). Dentre os principais problemas, destaca-se a questão da segurança cibernética, que atinge 22% dos usuários no país, refletindo o grau de exposição a ameaças digitais, mesmo em ambientes domiciliares.

Esse dado reforça a preocupação com a fragilidade das redes domésticas, a insuficiência de políticas de cibersegurança individual e a vulnerabilidade dos dispositivos utilizados fora das estruturas corporativas. A visualização demonstra a urgência de medidas proativas, tanto no nível institucional quanto pessoal, como o investimento em capacitação, adoção de boas práticas de segurança e o fortalecimento da infraestrutura digital.

Esse panorama impõe desafios significativos às autoridades, que muitas vezes não dispõem de estrutura, capacitação técnica ou legislação adequada para enfrentar a complexidade e a velocidade das ações criminosas no ciberespaço. O anonimato proporcionado por ferramentas como VPNs, proxies e criptografia, somado à operação em ambientes como a Deep Web, dificulta o rastreamento e a identificação dos autores dos crimes (SILVA; OLIVEIRA,

2021).

A investigação de crimes cibernéticos apresenta particularidades que a diferenciam dos crimes tradicionais, exigindo métodos investigativos especializados e adaptados ao ambiente digital. A natureza transnacional da internet e a ausência de fronteiras físicas aumentam a complexidade das apurações, uma vez que os agentes criminosos podem atuar anonimamente e a prova digital é extremamente volátil e suscetível a alterações (KERR, 2010; WALL, 2007).

Nesse contexto, a persecução penal no ambiente digital demanda uma atuação integrada e multidisciplinar, envolvendo unidades de polícia judiciária com expertise em tecnologia da informação, bem como uma cooperação eficaz entre instituições nacionais e internacionais (BLOOM, 2011; COLE, 2012). A preservação da cadeia de custódia das provas digitais é essencial para garantir sua validade em juízo e evitar nulidades processuais (BRASIL, 2012; NIST, 2020).

Diante desse cenário, destaca-se a importância de compreender o papel das autoridades envolvidas, os procedimentos técnicos e legais adotados, e as formas de colaboração entre os diversos atores. A criação de estruturas especializadas, como a Unidade Especial de Investigação de Crimes Cibernéticos (UEICC) da Polícia Federal, é um exemplo da necessidade de contar com equipes técnicas e humanas qualificadas, capazes de promover a cooperação entre órgãos públicos e privados e agilizar a troca de informações para fins de prevenção e repressão (POLÍCIA FEDERAL, 2023).

A complexidade dos crimes digitais exige ainda uma integração multidisciplinar entre profissionais das áreas de tecnologia, direito, psicologia, entre outras, além de uma cooperação internacional eficaz, capaz de superar obstáculos como a volatilidade das provas e a multiplicidade de jurisdições (MENDES; TORRES, 2020).

Este capítulo tem como objetivo analisar o papel das autoridades competentes, os procedimentos investigativos e as formas de colaboração na investigação dos crimes cibernéticos. Serão destacados os principais desafios enfrentados e as estratégias adotadas para aprimorar a eficácia das ações no ambiente digital. Compreender esses aspectos é fundamental para a construção de uma resposta institucional robusta e condizente com a realidade dinâmica e complexa do cibercrime (SANTOS, 2024).

2.2 Autoridades Envolvidas no Combate aos Crimes Cibernéticos

A Polícia Federal (PF) desempenha papel fundamental na investigação dos crimes

cibernéticos que possuem natureza federal e transnacional, conforme previsto no artigo 109, inciso V, da Constituição Federal, que estabelece sua competência para atuar em infrações penais que envolvam interesses da União ou que ultrapassem as fronteiras nacionais (Brasil, 1988). Essa atribuição é especialmente relevante diante do caráter global dos crimes digitais, que frequentemente envolvem conexões entre diferentes países e a violação de tratados internacionais, como a Convenção sobre Cibercrime de Budapeste, da qual o Brasil é signatário (Carvalho, 2022). A atuação da PF se destaca em casos em que a prática criminosa inicia-se no território nacional e seus efeitos se estendem para o exterior, ou vice-versa, configurando a chamada transnacionalidade, o que exige uma abordagem investigativa integrada e especializada (Silva; Oliveira, 2021).

No âmbito dos crimes cibernéticos, a Polícia Federal concentra esforços em investigações que envolvem fraudes bancárias internacionais, pirataria digital, ataques a sistemas governamentais e infraestruturas críticas, demonstrando sua capacidade técnica e operacional para enfrentar essas ameaças complexas. Exemplos recentes, como a Operação Redescobrimento, que desarticulou uma organização criminosa responsável pelo desvio de milhões de reais em contas no exterior, evidenciam a importância da cooperação internacional e da expertise da PF para o sucesso das investigações (Polícia Federal, 2023). Além disso, a criação da Unidade Especial de Investigação de Crimes Cibernéticos (UEICC), em 2022, representa um avanço significativo na consolidação de uma estrutura dedicada e qualificada para o rastreamento de provas digitais, incluindo dados voláteis e transações em criptomoedas, que são elementos essenciais para a elucidação dos delitos no ambiente virtual (Mendes; Torres, 2020).

A atuação da PF também se caracteriza pela intensa cooperação com órgãos internacionais, como a Europol e a UNC3T de Portugal, e pela parceria com instituições privadas, como a Federação Brasileira de Bancos (Febraban), para o compartilhamento de informações e o mapeamento de padrões criminosos, fortalecendo a resposta institucional frente à crescente sofisticação dos ataques (Santos, 2024). Contudo, permanecem desafios significativos, como os conflitos de jurisdição entre a esfera federal e estadual, que demandam a comprovação da efetiva transnacionalidade para que a PF possa atuar, conforme decisões recentes do Superior Tribunal de Justiça (STJ) (Carvalho, 2022). Além disso, as limitações legais para acesso a dados armazenados em servidores localizados em países sem acordos de cooperação dificultam a obtenção de provas essenciais para o processo investigativo (Silva; Oliveira, 2021).

Dessa forma, embora a Polícia Federal tenha ampliado sua capacidade técnica e

operacional para enfrentar os crimes cibernéticos de alcance federal e transnacional, a efetividade de sua atuação depende não apenas do aprimoramento das estruturas internas, mas também de avanços legislativos e do fortalecimento das parcerias internacionais. A complexidade e a dinâmica do cibercrime exigem uma resposta ágil, coordenada e integrada, que permita superar os obstáculos jurídicos e técnicos para garantir a segurança digital e a justiça (Mendes; Torres, 2020; Santos, 2024).

As Polícias Civis estaduais desempenham papel crucial na investigação dos crimes cibernéticos, por meio das delegacias especializadas que foram criadas para lidar com a complexidade e a especificidade dessas infrações no ambiente digital. Cada estado brasileiro pode contar com sua própria unidade ou departamento responsável por investigar delitos praticados pela internet e outros meios eletrônicos, como estelionato virtual, invasão de sistemas, roubo de identidade, disseminação de malware, entre outros (Advbox, 2024). Essas delegacias especializadas são compostas por agentes treinados em tecnologia da informação e técnicas específicas de investigação digital, utilizando ferramentas e softwares especializados para rastrear e analisar atividades ilícitas na internet, o que permite uma resposta rápida e eficaz aos crimes virtuais (Advbox, 2024).

Além da estrutura física e técnica, a capacitação contínua dos policiais civis é fundamental para o enfrentamento dos crimes cibernéticos. Programas de formação, como o curso promovido pela Secretaria de Defesa Social em Pernambuco, visam dotar os agentes de conhecimentos sobre aspectos legais, segurança da informação e procedimentos investigativos específicos para o ambiente digital, incluindo o entendimento das vulnerabilidades exploradas por hackers e crackers (SDS, 2024). Segundo especialistas, a investigação de crimes virtuais exige técnicas diferenciadas, pois os policiais precisam saber quais informações buscar e onde encontrá-las para atuar dentro dos parâmetros legais e garantir a proteção das vítimas (Wendt, 2024).

No âmbito investigativo, a Polícia Civil também tem se destacado no monitoramento e repressão a crimes digitais que envolvem apologia à violência, disseminação de conteúdos ilegais e exploração de vulneráveis, como demonstrado pela atuação da Delegacia Especializada em Repressão a Crimes Cibernéticos do Amazonas, que orienta a população sobre os crimes mais comuns e formas de denúncia (PC-AM, 2024). Em São Paulo, a Polícia Civil instaurou inquérito para investigar uma rede social por apologia à violência digital, ressaltando a importância da colaboração das plataformas digitais para o sucesso das investigações (SSP-SP, 2025).

Contudo, apesar dos avanços, as investigações de crimes cibernéticos enfrentam

desafios relacionados à necessidade de modernização da gestão policial, aquisição de aparatos tecnológicos adequados e a complexidade técnica dos delitos, que demandam uma atuação especializada e integrada entre os diversos órgãos de segurança pública (MPPI, 2022). A efetividade das investigações depende, portanto, da conjugação de recursos técnicos, capacitação contínua e cooperação institucional para superar as barreiras impostas pela natureza dinâmica e transnacional dos crimes digitais (MPPI, 2022).

No contexto da investigação dos crimes cibernéticos, diversas autoridades além das forças policiais desempenham papéis essenciais, como a Autoridade Nacional de Proteção de Dados (ANPD), o Banco Central e outros órgãos reguladores. A ANPD tem se destacado na fiscalização e investigação de incidentes envolvendo vazamentos e uso indevido de dados pessoais, protegidos pela Lei Geral de Proteção de Dados (LGPD). Desde o início da pandemia, a ANPD registrou um aumento de 300% nos casos relacionados à criminalidade cibernética, especialmente envolvendo dados pessoais dos cidadãos (ANPD, 2022). Em 2024, a ANPD intensificou sua atuação fiscalizatória, abrindo 31 processos de apuração de incidentes de segurança em apenas dez meses, número superior ao registrado nos quatro anos anteriores (O Globo, 2024). Embora sua atuação regulatória seja fundamental para a proteção dos dados, muitas vezes a ANPD interfere no andamento das investigações policiais ao priorizar processos administrativos, o que pode atrasar a atuação criminal e dificultar a integração entre os órgãos (Conjur, 2023).

O Banco Central do Brasil, por sua vez, exerce papel estratégico na investigação de fraudes financeiras digitais e ataques ao sistema bancário. Em parceria com a ANPD e as forças de segurança, o Banco Central regula e supervisiona as instituições financeiras para garantir a segurança das transações digitais e a proteção dos consumidores (ANPD, 2022). Entretanto, a atuação regulatória do Banco Central pode, por vezes, criar entraves burocráticos e limitações no compartilhamento ágil de informações com as autoridades policiais, o que compromete a rapidez das investigações e a resposta efetiva contra os criminosos (MPPI, 2022).

Outros órgãos reguladores, como a Comissão de Valores Mobiliários (CVM) e a Agência Nacional de Telecomunicações (Anatel), também participam do processo investigativo ao fiscalizar empresas e serviços que podem ser usados para práticas ilícitas, como fraudes em investimentos e ataques a redes de comunicação. No entanto, a falta de integração plena entre esses órgãos e as forças policiais frequentemente gera sobreposição de competências e atrasos na troca de informações, dificultando a condução eficiente das investigações (MPPI, 2022).

Essa interferência e fragmentação na atuação das autoridades envolvidas nas investigações de crimes cibernéticos evidenciam a necessidade urgente de aprimoramento dos

mecanismos de cooperação e coordenação entre os órgãos reguladores, a ANPD e as forças policiais. A ausência de um protocolo claro e ágil para o compartilhamento de informações e a definição de competências contribuem para a morosidade das investigações e para a impunidade dos criminosos digitais (Santos, 2024). Para superar esses desafios, é fundamental promover a integração institucional por meio de acordos de cooperação técnica, a criação de grupos interinstitucionais permanentes e a revisão das normas que regulam a atuação desses órgãos, garantindo que a proteção de dados e a regulação financeira não se sobreponham à necessidade de investigação criminal célere e eficaz (Mendes; Torres, 2020).

Assim, embora a ANPD, o Banco Central e os demais órgãos reguladores tenham papéis indispensáveis na prevenção e fiscalização dos crimes cibernéticos, sua atuação deve ser melhor alinhada com as forças policiais para que o processo investigativo seja mais eficiente e coordenado. Somente com essa integração será possível enfrentar com maior eficácia a complexidade dos crimes digitais e assegurar a segurança e a confiança no ambiente virtual (Santos, 2024).

2.3 Procedimentos na Investigação de Crimes Cibernéticos

O procedimento investigativo dos crimes cibernéticos inicia-se, em regra, com a notícia do fato, que pode ser formalizada por meio do boletim de ocorrência registrado pela vítima ou por terceiros que tenham conhecimento da infração. A partir dessa comunicação, a autoridade policial responsável deve avaliar a necessidade de instauração do inquérito policial para apurar a materialidade e autoria do delito, conforme previsto no Código de Processo Penal (CPP) brasileiro (Brasil, 1941). No âmbito dos crimes digitais, essa etapa é especialmente sensível, pois a preservação das provas digitais é urgente devido à sua natureza volátil e à facilidade de alteração ou destruição dos dados (CNJ, 2020).

Com a abertura do inquérito, a investigação deve seguir procedimentos técnicos específicos, orientados por protocolos como o estabelecido pelo Conselho Nacional de Justiça (CNJ), que determina a coleta e preservação adequada das evidências digitais, garantindo a integridade e a cadeia de custódia dos dados (CNJ, 2020). Entre as primeiras medidas investigativas destaca-se a solicitação de informações aos provedores de internet, que, conforme o Marco Civil da Internet (Lei nº 12.965/2014), devem fornecer dados cadastrais e registros de conexão mediante requisição das autoridades policiais, Ministério Público ou autoridades administrativas, sem a necessidade de ordem judicial para dados cadastrais, o que agiliza o processo (MPU, 2022).

A identificação do endereço IP utilizado no momento da prática do crime é um passo fundamental para localizar o autor e direcionar as diligências, como a expedição de mandados de busca e apreensão no local indicado, visando à confirmação da materialidade e à individualização da autoria (Franco, 2023). É imprescindível que esses mandados sejam específicos e abrangentes para evitar nulidades processuais, considerando a complexidade dos dispositivos eletrônicos investigados, como computadores pessoais, smartphones e outros equipamentos que armazenam grande volume de informações relevantes (MPU, 2022). A perícia forense digital, realizada por profissionais qualificados, é essencial para a análise técnica dos dados coletados, permitindo a extração de provas confiáveis que sustentem a acusação (Franco, 2023).

Além disso, a investigação deve considerar as particularidades dos crimes cibernéticos, como o uso de ferramentas de anonimato (VPNs, proxies, rede Tor) e a atuação em ambientes como a Deep Web, que dificultam o rastreamento dos autores. Para superar esses obstáculos, os investigadores utilizam técnicas avançadas de análise de tráfego de dados, correlação de informações e cooperação com provedores de serviços e órgãos internacionais (Crimes Digitais, 2025). A rapidez na obtenção e preservação das provas digitais é crucial, pois a demora pode resultar na perda irreparável de evidências, comprometendo a efetividade da investigação e a responsabilização dos criminosos (Franco, 2023).

Por fim, a investigação dos crimes cibernéticos demanda uma atuação integrada entre as diversas autoridades competentes, incluindo Polícia Civil, Polícia Federal, Ministério Público e órgãos reguladores, para garantir a celeridade e a eficácia do processo investigativo, respeitando os direitos fundamentais dos envolvidos e assegurando a segurança jurídica (CNJ, 2020; MPU, 2022). Dessa forma, o procedimento investigativo busca equilibrar a complexidade técnica dos delitos digitais com a necessidade de um processo justo e eficiente, fundamental para o combate à criminalidade virtual.

A coleta de dados é etapa fundamental no procedimento investigativo dos crimes cibernéticos, envolvendo requisições formais, rastreamento de endereços IP e geolocalização, que permitem identificar a autoria e a materialidade do delito. Inicialmente, a autoridade policial realiza requisições junto aos provedores de internet e serviços digitais para obtenção de registros de conexão e dados cadastrais, que, conforme o Marco Civil da Internet (Lei nº 12.965/2014), podem ser solicitados diretamente pelas autoridades policiais, Ministério Público ou órgãos administrativos, sem a necessidade de ordem judicial para dados cadastrais, o que agiliza o processo investigativo (MPU, 2022; CNJ, 2020). Esses registros, conhecidos como logs, são essenciais para mapear o histórico de acessos e identificar possíveis autores, especialmente

porque contêm informações como data, hora, endereço IP e tipo de conexão utilizada (Academia de Forense Digital, 2024).

O rastreamento do endereço IP é uma das ferramentas mais importantes para localizar a origem da atividade criminosa na internet. Através do IP, é possível identificar o provedor de conexão responsável pela atribuição daquele endereço no momento do crime, o que permite a solicitação de dados cadastrais do usuário associado (MPU, 2022). A partir desses dados, a autoridade pode determinar o local físico do suspeito, possibilitando a expedição de mandados de busca e apreensão para coleta de provas materiais e digitais, como computadores, smartphones e outros dispositivos eletrônicos (CNJ, 2020; Franco, 2023). A precisão e a especificidade desses mandados são essenciais para evitar nulidades processuais, especialmente diante da complexidade dos dispositivos investigados (MPU, 2022).

A geolocalização complementa o rastreamento do IP, fornecendo informações sobre a localização geográfica aproximada do usuário no momento da prática do crime. Essa técnica utiliza dados de torres de celular, GPS e outros sensores presentes nos dispositivos eletrônicos, auxiliando na confirmação da autoria e na delimitação territorial da investigação (Kroll, 2025). Contudo, a coleta e análise dessas informações exigem cuidados rigorosos para garantir a integridade e a cadeia de custódia das provas, preservando sua autenticidade para uso em processos judiciais (CNJ, 2020). Além disso, a atuação deve respeitar os direitos fundamentais, evitando abusos e garantindo a legalidade das medidas adotadas (MPU, 2022).

Em investigações mais complexas, a cooperação com provedores estrangeiros e órgãos internacionais é frequentemente necessária, especialmente quando os servidores que armazenam os dados estão localizados em outros países. Nesses casos, a obtenção das informações pode depender de tratados internacionais e mecanismos de cooperação jurídica, o que pode impactar a celeridade da investigação (MPU, 2022). Para minimizar esse impacto, algumas plataformas digitais mantêm canais específicos para atendimento a requisições judiciais e policiais, facilitando a preservação e o envio das evidências (Academia de Forense Digital, 2024; MPU, 2022).

Por fim, a coleta de dados em crimes cibernéticos deve ser realizada por profissionais capacitados, utilizando metodologias que garantam a integridade das informações e a conformidade legal, como previsto na norma ABNT NBR ISO/IEC 27037:2013. Essa atenção técnica é indispensável para que as provas digitais possam ser aceitas em juízo, contribuindo para a responsabilização efetiva dos autores e a segurança jurídica do processo (Academia de Forense Digital, 2024; Kroll, 2025). Assim, a combinação de requisições formais, rastreamento de IP e geolocalização compõe um conjunto estratégico para o sucesso das investigações em

crimes digitais.

As medidas cautelares constituem instrumentos indispensáveis no procedimento investigativo dos crimes cibernéticos, especialmente no que tange à quebra de sigilo telemático, fiscal e bancário, que são essenciais para a obtenção de provas e o sucesso da persecução penal. A quebra de sigilo telemático permite o acesso a dados armazenados em sistemas informatizados, como e-mails, mensagens e registros de conexão, possibilitando a identificação da autoria e a compreensão da dinâmica do delito (Fuller, 2021). Para que essas medidas sejam válidas, é imprescindível a autorização judicial, respeitando os direitos fundamentais previstos na Constituição Federal, garantindo que a interceptação e o acesso às informações sejam realizados dentro dos parâmetros legais (MPPI, 2021).

No âmbito do sigilo fiscal, a medida cautelar possibilita a requisição de informações junto à Receita Federal e demais órgãos tributários, para verificar movimentações financeiras suspeitas que possam estar relacionadas a crimes digitais, como lavagem de dinheiro e fraudes eletrônicas (MPPI, 2021). Já a quebra do sigilo bancário, autorizada judicialmente, permite o acesso a extratos, transferências e demais operações financeiras realizadas pelo investigado, sendo fundamental para rastrear recursos ilícitos e identificar conexões entre os envolvidos (Fuller, 2021). Essas medidas são complementares e, quando utilizadas de forma integrada, ampliam a capacidade investigativa das autoridades, contribuindo para a formação de um conjunto probatório robusto.

Recentemente, a legislação brasileira tem incorporado medidas cautelares específicas para crimes cibernéticos, como a proibição temporária de uso ou acesso à internet para acusados, prevista em projeto aprovado pela Comissão de Constituição e Justiça da Câmara dos Deputados, que visa impedir a continuidade da prática criminosa durante o processo investigativo (Câmara dos Deputados, 2023). Essa medida, que pode ser aplicada por até 15 dias, com possibilidade de prorrogação, demonstra a adaptação do ordenamento jurídico às particularidades dos crimes digitais, buscando equilibrar a proteção da ordem pública e os direitos individuais (Câmara dos Deputados, 2023).

Entretanto, a aplicação dessas medidas cautelares enfrenta desafios práticos, como a necessidade de rapidez na obtenção das autorizações judiciais para não comprometer a preservação das provas digitais, cuja volatilidade exige ações céleres (MPPI, 2021). Além disso, a complexidade técnica dos sistemas envolvidos demanda que as autoridades estejam preparadas para manejar as informações obtidas de forma segura e eficaz, evitando nulidades processuais e garantindo a integridade da cadeia de custódia (Fuller, 2021). A cooperação entre órgãos judiciais, policiais e reguladores é fundamental para o sucesso dessas medidas,

assegurando uma investigação coordenada e eficiente diante da transnacionalidade e sofisticação dos crimes cibernéticos (MPPI, 2021).

Dessa forma, as medidas cautelares de quebra de sigilo telemático, fiscal e bancário representam ferramentas estratégicas para a investigação criminal digital, sendo imprescindível seu uso fundamentado e equilibrado, respeitando os direitos constitucionais e promovendo a efetividade da justiça no combate aos delitos no ambiente virtual (Fuller, 2021; Câmara dos Deputados, 2023).

A busca e apreensão de dispositivos eletrônicos constituem etapas cruciais no procedimento investigativo dos crimes cibernéticos, pois permitem a coleta de evidências digitais indispensáveis para a comprovação da materialidade e autoria do delito. A autoridade judicial, ao receber a notícia do fato e a representação da autoridade policial ou do Ministério Público, pode determinar a expedição de mandado específico que autorize a apreensão dos equipamentos eletrônicos envolvidos, como computadores, notebooks, smartphones, pen drives e discos rígidos externos, conforme previsto no Código de Processo Penal e regulamentado por propostas legislativas recentes que visam garantir a correta custódia dos arquivos digitais (TJPB, 2024; Câmara dos Deputados, 2020). A precisão do mandado é fundamental para evitar nulidades, devendo conter detalhamento do local da diligência, os motivos da apreensão e a necessidade do acompanhamento de peritos em informática, garantindo o respeito à cadeia de custódia das provas (MPU, 2022; Câmara dos Deputados, 2020).

Durante a diligência, a apreensão pode ocorrer tanto pela remoção física dos dispositivos quanto pela produção de cópias forenses (espelhamento) dos dados armazenados, especialmente quando os equipamentos são volumosos ou essenciais para a continuidade das atividades do investigado. Essa técnica permite a análise detalhada do conteúdo sem comprometer o funcionamento dos aparelhos, preservando a integridade das provas (MPU, 2022). A intangibilidade da evidência digital torna sua destruição mais difícil, mas não impossível, razão pela qual a rapidez na execução da busca e apreensão é vital para evitar a perda ou alteração dos dados, que podem ser apagados ou corrompidos pelo investigado (MPU, 2022; Franco, 2023).

A análise técnica das evidências apreendidas é realizada por peritos especializados em informática forense, que aplicam metodologias e ferramentas específicas para recuperar, examinar e interpretar os dados digitais. Essa perícia é imprescindível para identificar vestígios deixados pelo autor do crime, como arquivos apagados, registros de acesso, comunicações eletrônicas e transações financeiras, assegurando a confiabilidade das provas para o processo judicial (Franco, 2023; MPU, 2022). Cabe destacar que, mesmo após a tentativa de exclusão de

arquivos, a perícia pode recuperar informações por meio de técnicas avançadas, reforçando a robustez da investigação (MPU, 2022).

Além disso, a busca e apreensão em crimes cibernéticos frequentemente requerem cooperação internacional, dada a possibilidade de os dados estarem armazenados em servidores localizados no exterior, o que demanda a utilização de mecanismos de cooperação jurídica internacional para garantir o acesso legal às informações (MPU, 2022). A atuação coordenada entre as autoridades policiais, judiciárias e periciais é essencial para assegurar que as evidências digitais sejam coletadas, preservadas e analisadas de forma adequada, respeitando os direitos fundamentais e a segurança jurídica (TJPB, 2024; Câmara dos Deputados, 2020).

Em suma, a busca e apreensão de dispositivos eletrônicos e a análise técnica das evidências digitais configuram procedimentos indispensáveis e complexos na investigação dos crimes cibernéticos, exigindo rigor técnico, legal e operacional para garantir a efetividade da persecução penal e a proteção dos direitos dos envolvidos (Franco, 2023; MPU, 2022).

A investigação dos crimes cibernéticos é um processo complexo que demanda procedimentos específicos e integrados para garantir a eficácia na apuração dos fatos e a responsabilização dos autores. O início da investigação, a partir da notícia do fato e da abertura do inquérito policial, é fundamental para formalizar a persecução penal e assegurar a preservação das provas digitais, que possuem natureza volátil e exigem atuação rápida e técnica (CNJ, 2020; Franco, 2023). A coleta de dados, por meio de requisições aos provedores, rastreamento de endereços IP e utilização da geolocalização, constitui uma etapa estratégica para identificar a autoria e delimitar o âmbito da investigação, sendo imprescindível o respeito aos direitos fundamentais e à legalidade das medidas adotadas (MPU, 2022; Academia de Forense Digital, 2024).

As medidas cautelares, especialmente as quebras de sigilo telemático, fiscal e bancário, são ferramentas essenciais para aprofundar a investigação, permitindo o acesso a informações protegidas que podem revelar a dinâmica dos crimes e os envolvidos. Contudo, sua aplicação requer autorização judicial e deve ser realizada com rigor técnico e jurídico para garantir a validade das provas e a segurança jurídica do processo (Fuller, 2021; Câmara dos Deputados, 2023). Por fim, a busca e apreensão de dispositivos eletrônicos, acompanhada da análise técnica das evidências por peritos especializados, completa o ciclo investigativo, possibilitando a recuperação e interpretação dos dados digitais que sustentam a acusação. Essa etapa demanda precisão, rapidez e cooperação entre os órgãos envolvidos para preservar a integridade das provas e assegurar a efetividade da justiça (Franco, 2023; MPU, 2022).

Assim, a conjugação desses procedimentos – desde a instauração do inquérito até a

análise técnica das evidências – demonstra a necessidade de uma atuação coordenada, especializada e célere no enfrentamento dos crimes cibernéticos. A complexidade técnica e a volatilidade das provas digitais impõem desafios que só podem ser superados por meio da integração entre autoridades policiais, judiciárias, periciais e regulatórias, respeitando os direitos constitucionais e promovendo a segurança jurídica. Dessa forma, o aprimoramento contínuo desses procedimentos é indispensável para fortalecer a resposta institucional frente à criminalidade digital e garantir a proteção da sociedade no ambiente virtual.

2.4 Cooperação Investigativa e Atuação Multissetorial

A cooperação investigativa e a atuação multissetorial são elementos fundamentais para o enfrentamento eficaz dos crimes cibernéticos, dada a complexidade técnica e a transnacionalidade dessas infrações. A integração entre a Polícia, o Ministério Público (MP), o Poder Judiciário e órgãos especializados permite a conjugação de competências, recursos e conhecimentos necessários para a investigação e repressão desses delitos. Conforme entendimento recente do Supremo Tribunal Federal (STF), o Ministério Público possui competência concorrente para conduzir investigações criminais, atuando de forma subsidiária à polícia judiciária e promovendo mecanismos de cooperação que fortalecem a persecução penal (STF, 2025; Migalhas, 2025).

Essa cooperação é formalizada por meio de acordos técnicos e protocolos que visam à capacitação conjunta, intercâmbio de dados e inteligência, além da proteção de informações sensíveis, conforme exemplificado pelo acordo firmado entre o Conselho Nacional do Ministério Público (CNMP) e a Polícia Federal. Tal parceria busca aprimorar a atuação integrada na área de inteligência, fortalecendo a capacidade investigativa e a eficácia no combate à criminalidade organizada e aos crimes cibernéticos (CNMP, 2022). A atuação coordenada entre esses órgãos também assegura o respeito aos direitos fundamentais, a observância do devido processo legal e a segurança jurídica durante as investigações, promovendo uma resposta institucional mais célere e eficiente (STF, 2025; Fachin, 2024).

Além disso, a integração multissetorial inclui a participação de órgãos reguladores, agências de inteligência e entidades privadas, que fornecem informações e suporte técnico imprescindíveis para a elucidação dos crimes digitais. O diálogo constante entre as instituições permite a superação de entraves burocráticos, a harmonização das competências e a otimização dos recursos disponíveis, configurando um modelo colaborativo indispensável para enfrentar a

sofisticação e a dinâmica dos crimes cibernéticos no Brasil (MPBA, 2023; Polícia Federal, 2023). Dessa forma, a cooperação investigativa e a atuação multissetorial consolidam-se como pilares estratégicos para a efetividade da justiça criminal em um cenário marcado pela complexidade tecnológica e pela necessidade de respostas integradas e coordenadas.

As forças-tarefas e os grupos interinstitucionais representam estratégias de atuação conjunta e coordenada para o enfrentamento dos crimes cibernéticos, reunindo expertise e recursos de diferentes órgãos e entidades. A Polícia Federal, por exemplo, tem apresentado projetos para a criação de forças-tarefas inéditas no país, visando unir esforços com grandes empresas e instituições financeiras no combate às ameaças cibernéticas. Essa iniciativa busca criar uma maior proteção dos dados pessoais e financeiros dos cidadãos, além de fortalecer a segurança nacional para atrair investimentos externos (Polícia Federal, 2022).

A criação de forças-tarefas possibilita a atuação conjunta de setores público e privado, visando tornar o espaço cibernético mais seguro e combater organizações criminosas que cometem crimes cibernéticos (Polícia Federal, 2022). No âmbito internacional, o Ministério das Relações Exteriores, em parceria com a Organização dos Estados Americanos (OEA) e o Institute For Security and Technology (IST), implementou a Força-Tarefa contra o Ransomware no Brasil (RTF Brasil), com o objetivo de fomentar discussões sobre os desafios enfrentados pela sociedade e o Estado brasileiro frente a esse tipo de crime (MRE, 2025). Essa força-tarefa reúne representantes de instituições estatais, privadas e da sociedade civil, buscando promover diagnósticos atualizados e discussões sobre possíveis formas de enfrentamento contra o ransomware (MRE, 2025).

As forças-tarefas têm se mostrado úteis no combate a crimes cibernéticos, sendo compostas, em regra, por peritos e investigadores altamente especializados (ESMPU, 2024). No Ministério Público Federal, são exemplos desse modo de atuação a Força-Tarefa do Caso Anaconda, de São Paulo, e a Força-Tarefa CC5 (também conhecida como Força-Tarefa do Banestado), que teve sede no Paraná e em Brasília (ESMPU, 2024). A utilização de forças tarefas como estratégia de combate à criminalidade organizada e aos atos de improbidade administrativa é indispensável nos dias atuais, permitindo resultados mais significativos do que a atuação exclusiva de uma determinada instituição ou a atuação isolada de um de seus membros (ESMPU, 2024).

Além das forças-tarefas, a criação de grupos interinstitucionais também fortalece a atuação conjunta no combate aos crimes cibernéticos. Esses grupos reúnem representantes de diferentes órgãos e entidades, como polícias, Ministérios Públicos, agências reguladoras e setor privado, para compartilhar informações, coordenar ações e desenvolver estratégias de

prevenção e repressão aos crimes digitais (Polícia Federal, 2022; MRE, 2025). A atuação integrada desses grupos permite uma resposta mais rápida e eficaz aos crimes cibernéticos, que exigem conhecimentos técnicos e jurídicos especializados, além de cooperação entre diferentes setores da sociedade.

Em suma, as forças-tarefas e os grupos interinstitucionais representam ferramentas importantes para o enfrentamento dos crimes cibernéticos, permitindo a união de esforços, o compartilhamento de informações e a coordenação de ações entre diferentes órgãos e entidades. A atuação conjunta e coordenada é fundamental para garantir a segurança cibernética e proteger a sociedade contra as ameaças digitais.

A cooperação internacional é elemento essencial no combate aos crimes cibernéticos, dada a natureza transnacional dessas infrações, que frequentemente envolvem atores, servidores e dados distribuídos em diferentes países. Organizações como a Interpol e a Europol desempenham papel central nesse contexto, atuando como pontos de convergência para o intercâmbio de informações, coordenação de operações conjuntas e apoio técnico às autoridades nacionais. A Interpol, por meio de sua Rede Global de Centros de Cooperação Cibernética, facilita a comunicação rápida entre países, promovendo a troca de inteligência e o suporte em investigações complexas que ultrapassam fronteiras (MPF, 2023; Polícia Federal, 2023). Já a Europol, com sua Unidade de Crimes Cibernéticos, oferece suporte operacional e analítico para os Estados-membros da União Europeia, além de estabelecer parcerias com países terceiros, incluindo o Brasil, fortalecendo a resposta internacional contra ameaças digitais (MPF, 2023).

Outro marco fundamental da cooperação internacional em matéria penal é a Convenção de Budapeste, adotada em 2001 e promulgada no Brasil em 2023, que constitui o primeiro tratado multilateral específico para o combate aos crimes cibernéticos. A Convenção estabelece diretrizes para a tipificação de delitos digitais, mecanismos de assistência jurídica mútua e procedimentos para a coleta e troca de provas eletrônicas entre os países signatários. Além disso, prevê salvaguardas para a proteção dos direitos humanos, buscando equilibrar a eficácia na repressão criminal com o respeito às garantias fundamentais (MPF, 2023; Rocha, 2023). A adesão do Brasil a esse tratado representa um avanço significativo, ampliando a capacidade das autoridades brasileiras de solicitar e prestar cooperação internacional de forma célere e segura, especialmente em investigações que envolvem provas digitais armazenadas no exterior (MPF, 2023).

Recentemente, a Organização das Nações Unidas (ONU) aprovou uma nova convenção global contra crimes cibernéticos, que visa fortalecer ainda mais os mecanismos de cooperação internacional, criando canais seguros e ágeis para a tramitação de pedidos de assistência mútua.

O Brasil teve papel ativo na negociação desse instrumento, reforçando seu compromisso com a colaboração internacional no enfrentamento da criminalidade digital. Essa convenção pretende ampliar a eficácia das investigações e a proteção das vítimas, especialmente em crimes graves como tráfico de pessoas, pedofilia e lavagem de dinheiro, que utilizam a internet como meio para sua prática (MJSP, 2024). Assim, a cooperação internacional, por meio da atuação conjunta da Interpol, Europol, da Convenção de Budapeste e dos novos instrumentos multilaterais, configura-se como pilar indispensável para o combate efetivo aos crimes cibernéticos, promovendo uma resposta global coordenada e integrada frente a um fenômeno que ultrapassa fronteiras nacionais.

A parceria entre órgãos públicos e empresas privadas, especialmente provedores de tecnologia, tem se mostrado fundamental para o enfrentamento dos crimes cibernéticos no Brasil. Iniciativas como a Aliança Nacional de Combate a Fraudes Digitais, coordenada pelo Ministério da Justiça e Segurança Pública (MJSP) em conjunto com a Federação Brasileira de Bancos (Febraban) e com a participação de empresas como o Serpro, exemplificam a importância da cooperação multissetorial para aprimorar a prevenção, detecção e repressão a golpes e fraudes digitais (MJSP, 2025; Serpro, 2025). Essa aliança promove o compartilhamento de informações, desenvolvimento de estratégias conjuntas e capacitação de agentes, fortalecendo a resposta institucional às ameaças cibernéticas e protegendo cidadãos, empresas e o setor público.

Além disso, a colaboração com provedores de serviços de internet e plataformas digitais é essencial para o rápido atendimento a requisições judiciais e policiais, como a disponibilização de logs, dados cadastrais e registros de conexão, que são cruciais para a identificação e localização dos autores de crimes virtuais (Conexis, 2025). O setor privado também contribui com investimentos em tecnologia e inovação, como laboratórios conjuntos de segurança cibernética, que treinam profissionais e realizam simulações para aprimorar a capacidade de resposta a ataques digitais (Febraban, 2024). Essas parcerias ampliam a capacidade técnica e operacional das autoridades, promovendo um ambiente digital mais seguro e confiável.

O ministro da Justiça e Segurança Pública, Ricardo Lewandowski, enfatiza que a inteligência, a capacitação técnica e a implementação de medidas integradas são as melhores formas de combater a criminalidade digital, destacando a necessidade de união entre os setores público e privado para enfrentar esse fenômeno crescente (MJSP, 2025). Dessa forma, a cooperação com empresas privadas e provedores de tecnologia não apenas potencializa as investigações, mas também contribui para a construção de políticas públicas eficazes e para a

conscientização da sociedade sobre os riscos e formas de proteção no ambiente virtual.

2.5 Colaboração Técnica nas Investigações

A participação de especialistas técnicos, como engenheiros, analistas e peritos forenses, é fundamental para o sucesso das investigações de crimes cibernéticos, dada a complexidade e a sofisticação das infrações digitais. A Polícia Federal, por exemplo, criou a Unidade Especial de Investigação de Crimes Cibernéticos (UEICC), que reúne profissionais altamente capacitados para atuar na análise técnica e na repressão a delitos praticados no ambiente virtual, como fraudes bancárias, ataques a sistemas governamentais e crimes contra instituições públicas e privadas (MJSP, 2022; Polícia Federal, 2023). Esses especialistas utilizam ferramentas avançadas para rastrear vestígios digitais, interpretar dados criptografados e reconstruir a dinâmica dos ataques, o que é imprescindível para identificar os autores e reunir provas robustas.

Além da Polícia Federal, outras instituições também contam com equipes técnicas especializadas, que incluem engenheiros de segurança da informação, analistas de dados e peritos em informática forense, capazes de realizar análises detalhadas de dispositivos eletrônicos e redes de comunicação. Esses profissionais aplicam metodologias específicas para garantir a integridade das provas digitais, como a criação de imagens forenses e o uso de algoritmos de hash para verificar a autenticidade dos dados coletados (Trend Micro, 2024; Advbox, 2023). A capacitação contínua desses especialistas é essencial para acompanhar a evolução das técnicas criminosas e as inovações tecnológicas, garantindo uma resposta rápida e eficiente às ameaças cibernéticas.

A colaboração técnica entre especialistas e as autoridades policiais também é facilitada por parcerias público-privadas, que promovem a troca de informações e o desenvolvimento conjunto de soluções para prevenção e investigação dos crimes digitais. A Federação Brasileira de Bancos (Febraban), por exemplo, criou laboratórios que simulam ataques cibernéticos e já capacitaram milhares de profissionais, compartilhando dados valiosos com a Polícia Federal para intensificar o combate às fraudes (MJSP, 2022). Dessa forma, a participação de engenheiros, analistas e peritos forenses é um componente estratégico indispensável para a eficácia das investigações, permitindo que as autoridades enfrentem com maior precisão e profundidade os desafios impostos pela criminalidade digital.

A colaboração técnica nas investigações de crimes cibernéticos tem se fortalecido significativamente por meio do apoio de núcleos técnicos especializados e parcerias com

universidades e centros de pesquisa. No âmbito do Ministério Público do Distrito Federal e Territórios (MPDFT), o Núcleo Especial de Combate aos Crimes Cibernéticos (Ncyber) oferece suporte qualificado às promotorias de justiça, atuando na análise técnica e no desenvolvimento de estratégias investigativas que envolvem conhecimento avançado em tecnologia da informação e segurança digital (MPDFT, 2025). Essa estrutura técnica permite que os membros do Ministério Público contem com expertise especializada, fundamental para a correta interpretação das evidências digitais e para a condução eficaz das investigações.

Paralelarmente, as parcerias com universidades e centros de pesquisa têm ampliado a capacidade investigativa e a inovação tecnológica no combate aos crimes virtuais. Instituições acadêmicas desenvolvem pesquisas focadas em segurança cibernética, análise forense digital, criptografia e inteligência artificial, que são aplicadas diretamente nas investigações criminais. Além disso, esses centros promovem a capacitação contínua de profissionais por meio de cursos, workshops e projetos conjuntos com órgãos públicos, como a Polícia Federal e o Ministério Público, fortalecendo o capital humano envolvido nas operações (MPMG, 2023; UFPel, 2024). Essa integração entre academia e poder público contribui para a atualização constante das metodologias investigativas e para o desenvolvimento de soluções técnicas adaptadas às novas ameaças digitais.

Outro exemplo dessa cooperação técnica é o Centro Integrado de Segurança Cibernética do Governo Digital (CISC Gov.br), que atua como uma unidade de coordenação operacional das equipes de prevenção, tratamento e resposta a incidentes cibernéticos nos órgãos públicos, promovendo interlocução com entidades privadas e órgãos especializados para apoio técnico e troca de informações (CISC Gov.br, 2023). Essa articulação multissetorial e multidisciplinar possibilita uma resposta mais ágil e eficaz diante dos desafios impostos pela criminalidade digital, ampliando o alcance e a profundidade das investigações. Assim, o apoio de núcleos técnicos e a parceria com universidades e centros de pesquisa são pilares estratégicos para o aprimoramento das investigações em crimes cibernéticos, garantindo maior eficiência, inovação e segurança jurídica no enfrentamento desse fenômeno.

A colaboração técnica entre órgãos públicos e empresas privadas especializadas em cibersegurança tem se mostrado cada vez mais essencial para o enfrentamento eficaz dos crimes cibernéticos no Brasil. A complexidade e a sofisticação das ameaças digitais exigem conhecimentos técnicos avançados e investimentos contínuos em tecnologia, recursos que muitas vezes ultrapassam a capacidade exclusiva do Estado. Nesse contexto, as parcerias público-privadas surgem como uma estratégia fundamental para ampliar a capacidade de prevenção, detecção e resposta a incidentes cibernéticos, promovendo a troca de informações,

o desenvolvimento conjunto de soluções e a capacitação de profissionais (INAC, 2023).

Um exemplo emblemático dessa cooperação é o acordo firmado em 2022 entre a Federação Brasileira de Bancos (Febraban) e o Ministério da Justiça e Segurança Pública, que visa o desenvolvimento de medidas preventivas, educativas e repressivas contra fraudes eletrônicas e ataques de alta tecnologia. Essa iniciativa demonstra a importância do setor privado na proteção dos dados e na segurança das operações financeiras, áreas frequentemente visadas por criminosos digitais (MJSP, 2025). Além disso, empresas do setor audiovisual têm colaborado com órgãos de investigação no combate à pirataria digital, contribuindo para ações de repressão que resultaram em operações de grande impacto, como a Operação 404 (INAC, 2023).

A colaboração com provedores de tecnologia e empresas especializadas também é crucial para o atendimento rápido e eficiente às requisições judiciais e policiais, como o fornecimento de logs, dados cadastrais e registros de conexão, que são fundamentais para a identificação e localização dos autores dos crimes virtuais. Essa parceria permite superar limitações técnicas e burocráticas, acelerando as investigações e fortalecendo a segurança digital (Agência Senado, 2024). Ademais, o setor privado investe em laboratórios e centros de pesquisa que promovem a inovação tecnológica e a capacitação de profissionais, ampliando a qualidade e a eficiência das respostas às ameaças cibernéticas (Febraban, 2024).

Em síntese, a colaboração entre o setor público e as empresas privadas especializadas em cibersegurança representa um pilar estratégico para a segurança digital no Brasil. Essa parceria fortalece a capacidade investigativa, amplia a proteção dos dados e sistemas e contribui para a construção de políticas públicas mais eficazes, promovendo um ambiente digital mais seguro e resiliente frente às crescentes ameaças do cibercrime (INAC, 2023).

2.6 Obstáculos à Persecução Cibernética

A investigação de crimes cibernéticos apresenta diversas dificuldades específicas, que a distinguem dos modelos tradicionais de persecução penal. Entre essas particularidades, destaca-se a proteção constitucional aos direitos fundamentais, como a intimidade, a privacidade e o sigilo das comunicações, que impõe barreiras legais e processuais à atuação investigativa. A necessidade de autorização judicial para obtenção de dados, a morosidade na resposta de entidades privadas, a volatilidade das provas digitais e a criptografia de ponta-a ponta são exemplos de obstáculos que comprometem a celeridade e a efetividade das

investigações. Tais entraves, aliados à crescente complexidade técnica dos delitos virtuais, exigem não apenas a qualificação dos agentes públicos envolvidos, mas também a modernização das estruturas institucionais e legislativas que regem o processo investigatório (Brasil, 1988; Brasil, 1941).

O primeiro desafio reside na própria natureza dos crimes cibernéticos, que são frequentemente praticados com o uso de dados falsos, linhas telefônicas habilitadas em nome de terceiros e aparelhos descartáveis. A demora na concessão de ordens judiciais para quebra de sigilo telefônico ou de dados de conexão pode tornar essas medidas inócuas, visto que os criminosos operam com grande agilidade e abandonam dispositivos ou contas após o cometimento do delito. Ainda, empresas responsáveis pela guarda de imagens ou informações relevantes costumam submeter os pedidos policiais à análise jurídica interna, o que contribui para o atraso no fornecimento de dados essenciais à identificação dos autores. Nesses casos, a lentidão pode comprometer toda a cadeia investigativa, resultando na perda de provas ou no insucesso da persecução penal (Caselli, 2022).

Além disso, a necessidade de autorização judicial para obtenção de informações como registros de IP, dados bancários e interceptações telefônicas representa outro obstáculo relevante. Embora tais medidas protejam os direitos fundamentais, o excesso de formalidades pode beneficiar os criminosos, que se valem dessas brechas temporais para escapar da responsabilização. A obtenção de diferentes dados em etapas sucessivas demanda múltiplos pedidos ao Poder Judiciário, o que amplia o tempo necessário para reunir elementos probatórios. Tal dinâmica é especialmente problemática em regiões onde não há juízes titulares disponíveis, sendo as decisões judiciais proferidas apenas uma vez por semana, o que pode atrasar em semanas a apuração de um simples golpe virtual (Duque, 2022; Freitas Junior; Lyra Neto, 2022).

Outro entrave recorrente está na falta de colaboração efetiva por parte das empresas detentoras das informações. Mesmo diante de ordens judiciais ou requisições legais baseadas no Marco Civil da Internet, não são raros os casos em que bancos, operadoras e provedores de internet demoram semanas para responder aos pedidos, alegando sobrecarga de seus departamentos jurídicos. Essa resistência, ainda que compreensível diante do alto volume de demandas, representa uma grave ameaça à efetividade das investigações. A situação é agravada pela necessidade de reiterações constantes e pela inexistência de canais diretos e atualizados de comunicação entre os órgãos de segurança pública e as empresas detentoras dos dados (Freitas, 2021; Brasil, 2013; Brasil, 2014).

A criptografia de ponta-a-ponta, especialmente utilizada em aplicativos de mensagens

como o WhatsApp, representa um dos principais desafios enfrentados pelas autoridades investigativas. A impossibilidade de interceptar o conteúdo de mensagens e ligações realizadas por meio dessas plataformas impede a obtenção de provas relevantes, ainda que haja autorização judicial. Essa limitação tem sido explorada por criminosos cibernéticos, que optam por se comunicar exclusivamente por esses meios, sabendo da inviabilidade técnica de monitoramento. Assim, mesmo diante de mandados judiciais, o conteúdo das comunicações permanece inacessível, prejudicando a elucidação dos fatos e a responsabilização dos agentes (Caselli, 2022).

Outro fator crítico é a falta de softwares especializados e atualizados para a extração de dados de dispositivos apreendidos. Mesmo com ferramentas como o Cellebrite, muitos aparelhos permanecem inacessíveis devido a senhas, criptografias e atualizações de sistema operacional. A alta demanda e o custo elevado dessas tecnologias fazem com que os órgãos de investigação disponham de poucos centros de extração de dados, resultando em longas filas e atrasos que, em muitos casos, inviabilizam a utilização das provas dentro do prazo processual. Não são raras as situações em que os dados extraídos chegam às delegacias após o término do processo judicial, sem utilidade prática para a responsabilização penal (Caselli, 2022; Duque, 2022).

As dificuldades se agravam ainda mais quando consideradas as distâncias geográficas entre os envolvidos nos crimes virtuais. Por se tratarem de delitos praticados por meio da internet, não é comum que vítima e autor estejam na mesma jurisdição, o que acarreta a necessidade de expedição de cartas precatórias para oitivas, diligências e buscas e apreensões. Esses pedidos, muitas vezes, levam meses ou anos para serem cumpridos e devolvidos aos autos, retardando ainda mais o andamento do inquérito. Além disso, a execução de medidas em outra jurisdição depende da atuação de policiais que não têm conhecimento direto dos detalhes do caso, o que pode comprometer a eficácia das diligências (Duque, 2022; Freitas Junior; Lyra Neto, 2022).

A cooperação internacional também se apresenta como um desafio expressivo, especialmente em casos que envolvem agentes localizados fora do país ou servidores estrangeiros. Embora o Brasil tenha aderido à Convenção de Budapeste, os mecanismos de colaboração previstos, como a Rede 24/7, ainda não estão plenamente implementados no país, sendo necessário recorrer a cartas rogatórias ou à intermediação do Ministério Público Federal. Tais procedimentos são, por natureza, lentos e burocráticos, o que dificulta o acesso rápido a provas armazenadas em território estrangeiro e reduz as chances de sucesso das investigações transnacionais (Council of Europe, 2023; MJSP, 2024).

Também há indefinições quanto à competência jurisdicional para julgamento dos crimes cibernéticos, o que impacta diretamente a condução das investigações. A jurisprudência e a legislação têm evoluído para tentar sanar essas controvérsias, como no caso do estelionato, cuja competência foi recentemente fixada pelo local do domicílio da vítima. No entanto, em outros crimes, como o furto eletrônico, ainda existem divergências quanto ao foro competente, o que gera conflitos de competência e paralisa investigações em andamento. A definição de competência é ainda mais desafiadora em casos que envolvem múltiplas vítimas, contas bancárias em diferentes localidades ou empresas públicas federais, exigindo a atuação da Polícia Federal e da Justiça Federal (Brasil, 2021; STJ, 2022).

Por fim, destaca-se a insuficiência de unidades especializadas no combate aos crimes cibernéticos. Embora a pandemia tenha impulsionado o aumento exponencial dessas infrações, o mesmo não ocorreu em relação à criação de estruturas investigativas adequadas. Muitas regiões do país ainda não contam com delegacias especializadas ou profissionais treinados para lidar com delitos dessa natureza. A falta de investimentos em tecnologia, capacitação e estrutura compromete a qualidade das investigações e contribui para o elevado índice de arquivamentos sem elucidação (Ferreira, 2022; Duque, 2022).

Frente a esse cenário, uma das soluções mais promissoras seria a criação de um órgão nacional centralizado de investigação cibernética, composto por representantes das Polícias Civis de todos os Estados e do Distrito Federal. Essa agência teria como objetivo a unificação das investigações, o compartilhamento de dados, a padronização dos procedimentos operacionais e a concentração dos pedidos de quebra de sigilo em uma vara especializada, com atuação célere e técnica. A centralização também permitiria economia de recursos e otimização da infraestrutura tecnológica, como a aquisição conjunta de softwares e equipamentos especializados (Caselli, 2022; Duque, 2022).

Essa estrutura nacional poderia operar de forma remota, com equipes espalhadas pelo território nacional e conectadas por canais seguros de comunicação, garantindo diligências rápidas e eficazes em qualquer parte do país. A integração das bases de dados, a criação de um cadastro de criminosos e a definição de um procedimento padrão de investigação contribuíram para aumentar a taxa de resolução dos casos e reduzir a sensação de impunidade. Embora essa solução não resolva todos os problemas — como a criptografia ponta-a-ponta —, ela representa um passo concreto em direção a um sistema investigativo mais moderno, eficiente e coordenado (Freitas, 2021; Freitas Junior; Lyra Neto, 2022).

2.7 Considerações Finais

A investigação de crimes cibernéticos representa, na atualidade, um dos maiores desafios para o sistema de justiça penal, exigindo não apenas atualização tecnológica, mas também reestruturação normativa, integração institucional e especialização técnica. A análise empreendida ao longo deste trabalho revelou um cenário marcado por entraves substanciais à efetividade investigativa, decorrentes, sobretudo, da natureza transnacional e altamente volátil das infrações digitais, da necessidade de múltiplas autorizações judiciais, da escassez de recursos humanos e materiais especializados, bem como da ineficiência de determinados fluxos procedimentais.

Constatou-se, ainda, que a investigação dos crimes cibernéticos demanda um modelo de atuação pautado pela colaboração multissetorial. A cooperação entre os diversos órgãos do sistema de justiça — Polícia Civil, Polícia Federal, Ministério Público, Poder Judiciário —, bem como a articulação com entidades reguladoras, universidades, centros de pesquisa e empresas privadas especializadas em tecnologia, constitui elemento imprescindível à superação das dificuldades impostas pelas especificidades técnicas dessas infrações. A atuação integrada permite não apenas maior agilidade na coleta e preservação de provas digitais, mas também o aprimoramento dos métodos investigativos e a redução de duplicidades operacionais.

Nesse contexto, a proposta de criação de um órgão centralizado, de caráter nacional, voltado exclusivamente à investigação de crimes cibernéticos, revela-se como alternativa viável e promissora. A centralização de competências, a padronização de procedimentos, o compartilhamento de dados em tempo real e a consolidação de canais diretos com provedores de tecnologia e instituições bancárias representariam avanços significativos na resposta estatal à criminalidade digital. Tal estrutura permitiria, ainda, a racionalização do uso de recursos, a atualização contínua de ferramentas tecnológicas e a formação de uma base de dados nacional de investigados e métodos utilizados, favorecendo a atuação preventiva e repressiva.

Importa destacar, por fim, que a proteção da sociedade frente aos delitos informáticos não poderá ser alcançada sem o fortalecimento do aparato investigativo estatal. Enquanto persistir a escassez de unidades especializadas, a indefinição jurisdicional, a morosidade procedimental e a ausência de soluções para a interceptação de comunicações criptografadas, a impunidade seguirá alimentando a expansão dessas condutas ilícitas. É imperioso, portanto, que sejam adotadas medidas estruturantes que articulem inovação, legalidade, eficiência e respeito aos direitos fundamentais. Somente assim será possível reverter o atual quadro de fragilidade institucional diante dos crimes cibernéticos e assegurar uma tutela penal compatível com os desafios da era digital.

CAPÍTULO III
CASOS PRÁTICOS E PRECEDENTES JURÍDICOS

3.1 Casos relevantes de Estelionato Cibernético

O estelionato cibernético, também denominado fraude eletrônica, consolidou-se como uma das modalidades criminosas de maior crescimento e impacto no Brasil nos últimos anos, tanto pela frequência com que é praticado quanto pela magnitude dos prejuízos financeiros que causa. Dados recentes apontam que, apenas entre 2021 e 2022, houve um aumento de 66% nas ocorrências registradas, totalizando 200.322 casos no último ano, número que representa um salto exponencial quando comparado à década anterior (FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA, 2023). Em termos de incidência geográfica, observa-se uma concentração particularmente elevada nos estados de Santa Catarina, Minas Gerais, Distrito Federal e Espírito Santo, sendo que Santa Catarina, isoladamente, responde por cerca de um quarto dos registros nacionais (MARQUES, 2023). Esse cenário reflete não apenas o aumento do uso de tecnologias digitais e da migração das relações pessoais e comerciais para o ambiente virtual — intensificada pela pandemia de COVID-19 —, mas também a sofisticação crescente das estratégias criminosas e a dificuldade das forças policiais em acompanhar a escalada e a diversidade das ocorrências (FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA, 2023).

Entre as modalidades mais recorrentes, destaca-se o golpe da clonagem de contas no aplicativo WhatsApp, que consiste na apropriação indevida do perfil da vítima, permitindo ao criminoso se passar por ela para solicitar transferências de valores a familiares, amigos e contatos profissionais. A credibilidade que a identidade verdadeira da vítima confere à abordagem torna o golpe extremamente eficaz, pois explora diretamente a confiança pessoal (MARQUES, 2023).

Em 2020, por exemplo, o humorista Rafael Portugal e sua esposa foram vítimas de um sofisticado esquema de pirâmide financeira com criptomoedas, disseminado pela empresa GAS Consultoria Bitcoin, liderada por Glaidson Acácio dos Santos, conhecido como o “Faraó dos Bitcoins”. Entre agosto de 2020 e março de 2021, o casal realizou seis aportes, totalizando aproximadamente R$ 1,2 milhão, atraídos por contratos que prometiam 10% de lucro mensal . O esquema foi desbaratado pela Operação Kryptus, conduzida pela Polícia Federal, que identificou movimentações de bilhões de reais e a prática fraudulenta de pirâmide financeira . Posteriormente, o casal ajuizou ação judicial visando o ressarcimento integral, e foi deferido o arresto cautelar de R$ 1,4 milhão em bens da empresa, abrangendo o valor inicial, correção

monetária e juros.

Outro esquema bastante difundido envolve fraudes em plataformas de compra e venda online, nas quais perfis falsos oferecem produtos inexistentes ou muito abaixo do preço de mercado, atraindo vítimas para pagamentos antecipados ou negociações manipuladas. Um exemplo relevante é a Operação *Broker Phanthom*, deflagrada pela polícia em diversos estados brasileiros para desarticular um esquema conhecido como "falso intermediário", no qual tanto o comprador quanto o vendedor eram vítimas. Nesse golpe, os criminosos criavam anúncios falsos de veículos e se apresentavam como intermediários, instruindo as partes a não discutirem valores enquanto conduziam a fraude. A investigação revelou que mais de 100 anúncios falsos foram responsáveis por um prejuízo de aproximadamente R$ 1,8 milhão, além do bloqueio judicial de 1.776 contas bancárias e do sequestro de bens avaliados em mais de R$ 600 mil. Segundo o delegado Murilo Freire, esses valores e bens poderão ser destinados ao ressarcimento das vítimas (G1, 2024).

Os golpes de *phishing*, disseminados via e-mail, SMS e aplicativos de mensagem, continuam ocupando posição de destaque, explorando a ingenuidade ou distração do usuário para levá-lo a páginas falsas que reproduzem a aparência de sites legítimos de instituições financeiras, órgãos governamentais ou grandes empresas. Nessas páginas fraudulentas, dados sensíveis como senhas, números de cartão e códigos de autenticação são coletados e usados para subtrair recursos ou assumir o controle de contas bancárias. Em um formato mais sofisticado dessa mesma técnica, têm se popularizado as chamadas falsas centrais de atendimento, nas quais criminosos entram em contato com a vítima se passando por funcionários de bancos ou empresas de tecnologia, induzindo-a a fornecer informações sigilosas ou a instalar aplicativos de acesso remoto em seu celular ou computador (MARQUES, 2023). Um caso amplamente divulgado ocorreu em 2022, quando clientes do Banco do Brasil foram alvo de um golpe em que recebiam ligações falsas sobre "movimentações suspeitas" e, induzidos a seguir instruções, acabavam permitindo que os fraudadores acessassem suas contas e transferissem valores elevados (BANCO DO BRASIL, 2022).

Ainda, uma situação semelhante foi relatada pela Federação Brasileira de Bancos (Febraban) em 2024, envolvendo o chamado golpe da falsa central telefônica, no qual criminosos utilizam gravações que simulam as Unidades de Resposta Audível (URA) dos bancos para conferir credibilidade à fraude. Assim como no caso do Banco do Brasil, a abordagem começa com o aviso sobre uma suposta compra ou transação suspeita, direcionando a vítima a um falso atendente. Este, por sua vez, solicita a instalação de aplicativos de acesso remoto, o fornecimento de senhas e dados pessoais ou a realização de transferências para contas

de terceiros, sob o pretexto de “regularizar” o problema. Em algumas variações, mensagens de texto, e-mails ou contatos por redes sociais reforçam a falsa narrativa. A Febraban reforça que instituições financeiras jamais solicitam esse tipo de informação ou transação por telefone e orienta que, diante de contatos suspeitos, o cliente desligue imediatamente e entre em contato com os canais oficiais do banco (FEBRABAN, 2024).

Casos de grande repercussão reforçam a percepção de que o estelionato cibernético não se limita a fraudes pontuais, mas constitui um fenômeno estruturado e altamente organizado. Casos e grande repercussão reforçam a percepção de que o estelionato cibernético não se limita a fraudes pontuais, mas constitui um fenômeno estruturado e altamente organizado. Um exemplo emblemático foi a Operação BitTrack, deflagrada pela Polícia Civil de Santa Catarina em outubro de 2024, que desarticulou uma organização criminosa especializada em fraudes bancárias envolvendo gerenciadores financeiros. A investigação revelou um esquema sofisticado que desviava recursos de uma prefeitura catarinense, utilizando contas de laranjas para converter valores em Bitcoins e transferi-los para carteiras privadas na blockchain, com o intuito de dificultar o rastreamento e ocultar a origem ilícita. Graças a ferramentas avançadas de análise, como a tecnologia da Chainalysis, foi possível rastrear os ativos digitais e vincular as carteiras à cúpula da organização, que já possuía antecedentes por crimes semelhantes. A operação contou com a participação integrada de diversas forças policiais e órgãos de inteligência nacionais, resultando na apreensão de bens, bloqueio de contas bancárias e sequestro de criptoativos, evidenciando a importância da cooperação interestadual e do uso de tecnologia no combate ao crime organizado (POLÍCIA CIVIL, 2024).

Outro exemplo, relevante é a Operação Open Doors, deflagrada inicialmente em agosto de 2017, que revelou a atuação de uma organização criminosa altamente estruturada responsável por fraudes bancárias em diversos estados brasileiros, como Rio de Janeiro, Santa Catarina, São Paulo, Paraná, Pará e Bahia. Segundo o Ministério Público do Estado do Rio de Janeiro, o grupo operou por cerca de uma década, desviando apenas entre 2016 e 2017 mais de R$ 30 milhões por meio da invasão de contas bancárias e transferência eletrônica dos valores para contas de laranjas. As investigações também apontaram práticas de lavagem de dinheiro, incluindo a aquisição de bens de alto valor como lanchas, jet skis e imóveis, registrados em nome de terceiros para ocultar a origem ilícita dos recursos. A complexidade e a longevidade da atuação criminosa evidenciam o grau de especialização dos envolvidos e a necessidade de operações coordenadas e interestaduais para o enfrentamento desse tipo de delito (G1, 2019).

O aspecto transnacional de muitas dessas operações impõe obstáculos adicionais à investigação. A atuação a partir de jurisdições conhecidas por sua resistência à cooperação

jurídica internacional, aliada ao uso de tecnologias de anonimização como redes privadas virtuais (VPN) e o navegador Tor, dificulta sobremaneira a identificação dos autores e a preservação das provas digitais. Essa dinâmica criminal é marcada por velocidade e volatilidade: em muitos casos, a fraude é cometida em questão de horas e os recursos transferidos são rapidamente pulverizados em múltiplas contas ou convertidos em ativos digitais de difícil rastreamento (FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA, 2023).

Do ponto de vista jurídico, o estelionato é tipificado pelo artigo 171 do Código Penal, que descreve a conduta de obter vantagem ilícita em prejuízo alheio, induzindo ou mantendo alguém em erro por meio de artifício ou ardil. A crescente incidência de fraudes eletrônicas motivou a edição da Lei nº 14.155/2021, que introduziu no dispositivo o §2º-A, qualificando o estelionato eletrônico e prevendo pena de reclusão de quatro a oito anos, além de multa (BRASIL, 2021). A inclusão dessa qualificadora representou um avanço no reconhecimento da gravidade do delito quando cometido por meios digitais, estabelecendo sanção mais severa do que a prevista para o estelionato comum. O §2º-B e o §3º, por sua vez, preveem agravantes específicas quando o crime é praticado mediante o uso de servidor no exterior ou quando tem como alvo entidades públicas, refletindo a preocupação com a dimensão transnacional e institucional dessas fraudes (BRASIL, 2021).

3.2 Análise de Julgados e o seu Impacto na Investigação dos Crimes Cibernéticos

A atuação do Supremo Tribunal Federal (STF) e do Superior Tribunal de Justiça (STJ) tem desempenhado papel central na conformação do aparato jurídico voltado à repressão e investigação do estelionato cibernético no Brasil. Não se trata apenas de interpretar e aplicar dispositivos legais existentes, mas de adaptar o sistema processual penal às peculiaridades dos delitos digitais, nos quais a volatilidade das provas, a velocidade da execução e a possível transnacionalidade das condutas impõem desafios inéditos às autoridades. Assim, os precedentes judiciais têm funcionado como vetores de orientação para a polícia judiciária, o Ministério Público e até mesmo para os órgãos reguladores, moldando práticas investigativas e definindo responsabilidades de terceiros, como instituições financeiras e provedores de serviços digitais.

Um marco relevante foi a decisão do STF no Inquérito 4.781/DF, de 2021, que reconheceu a natureza permanente dos crimes cometidos no ambiente virtual. Ao considerar que condutas ilícitas praticadas na internet permanecem disponíveis e acessíveis por tempo indeterminado, a Corte firmou entendimento de que esses delitos mantêm-se em estado de

consumação contínua. Essa posição repercute diretamente nas investigações, ao ampliar a possibilidade de reconhecimento do estado de flagrante, permitindo atuação mesmo após dias ou semanas da prática inicial do ato (BRASIL, STF, Inquérito 4781/DF, 2021).

Ainda, as decisões recentes do ministro Alexandre de Moraes no STF expandem significativamente o alcance das investigações sobre crimes digitais, estabelecendo a responsabilidade das plataformas digitais por conteúdos ilegais relacionados a organizações criminosas e milícias digitais (STF, 2025). Nessas decisões, foram autorizadas quebras de sigilo telemático, bloqueios massivos de contas e perfis falsos, e ordens para remoção de conteúdos que incitam a prática de crimes ou atentam contra instituições democráticas. Um aspecto relevante é que essas medidas, embora não tratem exclusivamente de estelionato eletrônico, estabelecem parâmetros de cooperação obrigatória para plataformas e provedores, o que beneficia diretamente investigações de fraudes virtuais ao obrigar empresas de tecnologia a fornecer dados de identificação e registros de acesso de forma célere (AGÊNCIA BRASIL, 2024).

O STJ, por sua vez, tem consolidado entendimentos que influenciam diretamente a efetividade da persecução penal. Entre eles, destaca-se a jurisprudência sobre competência jurisdicional em crimes digitais, assegurando que a investigação seja conduzida no foro adequado, evitando a anulação de atos processuais e a perda de tempo investigativo (BRASIL, STJ, decisão, 2022). A Corte também tem definido critérios para a admissibilidade de provas digitais, exigindo a observância de protocolos técnicos que garantam a integridade e autenticidade das evidências, como a cadeia de custódia prevista no Código de Processo Penal (BRASIL, STJ, 2018). A jurisprudência do STJ também tem reiterado que provas digitais obtidas sem autorização judicial violam direitos fundamentais previstos no art. 5º, X, da Constituição Federal, sendo, portanto, inadmissíveis no processo penal. Tal entendimento reforça a necessidade de observância estrita aos procedimentos legais para garantir a validade das provas, especialmente em crimes cibernéticos, onde a coleta e preservação do material probatório exigem rigor técnico e jurídico (BRASIL, STJ, 2018).

Essas medidas impactam o ambiente investigativo ao ampliar a atuação judicial nas redes sociais e demais ambientes virtuais, aumentando a capacidade de rastreamento de fraudes, desmantelamento de esquemas e identificação de autores.

Outro ponto relevante é que tanto o STF quanto o STJ têm consolidado o entendimento de que, para fins de competência processual, o local de consumação do delito digital, como no caso do estelionato eletrônico, é aquele onde o dano foi efetivamente sofrido pela vítima. Esse critério facilita a delimitação jurisdicional e acelera as investigações, evitando disputas de

competência e garantindo maior eficiência na tramitação processual.

Esses precedentes, somados, demonstram que a adaptação do sistema jurídico aos crimes cibernéticos vai além da criação de tipos penais específicos, como o §2º-A do art. 171 do Código Penal (introduzido pela Lei nº 14.155/2021). Trata-se de uma reestruturação investigativa que reconhece as particularidades do ambiente digital: a efemeridade das provas, o uso de tecnologias de anonimização, a multiplicidade de jurisdições envolvidas e a necessidade de ações simultâneas em diferentes frentes. Decisões do STF e STJ têm, portanto, contribuído para fortalecer a investigação do estelionato cibernético ao ampliar as hipóteses de flagrante e permitir intervenções mais efetivas, definir regras claras de competências e de admissibilidade de provas digitais, impor deveres de cooperação a empresas privadas e reforçar a corresponsabilidade preventiva de instituições financeiras e plataformas digitais.

Esse arcabouço jurisprudencial, ainda em construção, evidencia um esforço das cortes superiores para alinhar a proteção das garantias fundamentais com a necessidade de uma resposta estatal célere e eficaz, criando um ambiente normativo mais favorável à identificação, responsabilização e punição de autores de fraudes eletrônicas no Brasil.

CONCLUSÃO

O presente estudo abordou a complexa temática da investigação de crimes cibernéticos no Brasil, com ênfase no estelionato digital, destacando a relevância crescente dessa modalidade criminosa no cenário contemporâneo. Foi possível constatar que a transformação digital, ao mesmo tempo em que ampliou as oportunidades de interação, comércio e inovação, também potencializou vulnerabilidades exploradas por agentes mal-intencionados, que se valem do ambiente virtual para aplicar golpes sofisticados e de difícil rastreamento.

Ao longo da pesquisa, verificou-se que o estelionato digital, previsto no art. 171, §2º-A, do Código Penal, tem se expandido de forma preocupante, impulsionado pelo uso de tecnologias de anonimização, pela transnacionalidade das condutas e pela volatilidade das provas digitais. As estatísticas analisadas evidenciam não apenas um crescimento expressivo de ocorrências, mas também prejuízos financeiros bilionários e impactos sociais relevantes, atingindo vítimas em todo o território nacional.

A investigação desses delitos enfrenta barreiras significativas, como a morosidade processual, a dificuldade de cooperação com provedores de serviços, a necessidade de múltiplas autorizações judiciais e a insuficiência de unidades especializadas em determinadas regiões. O uso de criptografia ponta-a-ponta e a hospedagem de dados no exterior agravam o cenário, dificultando a coleta de provas e exigindo mecanismos de cooperação internacional mais céleres e eficientes.

Os casos e precedentes analisados demonstraram que as cortes superiores, especialmente o Supremo Tribunal Federal (STF) e o Superior Tribunal de Justiça (STJ), têm desempenhado papel fundamental na adaptação do aparato jurídico às particularidades dos crimes digitais. Decisões que ampliam hipóteses de flagrante, definem critérios de competência territorial, reforçam a validade de provas digitais obtidas conforme a cadeia de custódia e estabelecem deveres de cooperação para instituições financeiras e plataformas tecnológicas contribuem para fortalecer o processo investigativo.

Verificou-se, ainda, que a efetividade no combate ao estelionato digital depende de uma atuação integrada e multissetorial, envolvendo Polícia Federal, Polícias Civis, Ministério Público, Poder Judiciário, órgãos reguladores, empresas privadas e especialistas técnicos. A experiência de forças-tarefas, grupos interinstitucionais e parcerias público-privadas revela que a cooperação pode reduzir entraves burocráticos, acelerar o compartilhamento de informações e aprimorar a capacidade de resposta do Estado frente a ameaças cibernéticas cada vez mais complexas.

Assim, restou evidente que a modernização da legislação, a ampliação de estruturas especializadas, o investimento em tecnologia e capacitação, e o fortalecimento da cooperação nacional e internacional são medidas imprescindíveis para tornar mais eficaz a persecução penal dos crimes cibernéticos. Ao mesmo tempo, é essencial que tais avanços sejam acompanhados da preservação dos direitos e garantias fundamentais, assegurando que a proteção da sociedade ocorra dentro dos limites constitucionais.

Portanto, a investigação do estelionato digital exige uma abordagem equilibrada, que una rigor técnico, celeridade processual, integração institucional e respeito à legalidade. Somente com um aparato investigativo robusto e adaptado às especificidades do ambiente virtual será possível mitigar os riscos, reduzir a impunidade e garantir a segurança e a confiança nas relações digitais no Brasil.

REFERÊNCIAS

ACADEMIA DE FORENSE DIGITAL. Coleta de evidências digitais. 2024. Disponível em: https://academiadeforensedigital.com.br/. Acesso em: 13 jun. 2025.

ADVBOX. Delegacias especializadas em crimes cibernéticos. 2024. Disponível em: https://advbox.com.br/blog/delegacia-de-cibercrimes/. Acesso em: 13 jun. 2025.

AGÊNCIA BRASIL. Entenda decisão de Moraes que ampliou investigações digitais. Brasília, 2024. Disponível em: https://agenciabrasil.ebc.com.br/justica/noticia/2024-04/entenda-decisao-de-moraes-que-incluiu-musk-em-investigacao-no-stf. Acesso em: 7 ago. 2025.

AGÊNCIA SENADO. Cooperação com empresas de tecnologia no combate ao cibercrime. 2024. Disponível em: https://www12.senado.leg.br/noticias/materias/2024/07/11/ciberseguranca-deve-ter-agencia-estatal-com-parceria-privada-conclui-debate. Acesso em: 13 jun. 2025.

ANPD. Relatório de Atividades 2022. Brasília: Autoridade Nacional de Proteção de Dados, 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes. Acesso em: 13 jun. 2025.

BANCO DO BRASIL. Golpe da falsa central de atendimento: modus operandi e orientações para prevenção. Brasília, 2022. Disponível em: https://blog.bb.com.br/golpe-da-falsa-central/. Acesso em: 7 ago. 2025.

BLOOM, R. Digital forensics in cybercrime investigations. Journal of Cyber Security, v. 3, n. 2, p. 45-60, 2011. Disponível em: https://scholar.google.com/. Acesso em: 13 jun. 2025.

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Brasília, DF: Presidência República, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 13 jun. 2025.

BRASIL. Decreto-Lei nº 3.689, de 3 de outubro de 1941. Código de Processo Penal.

Brasília, DF: da República, 1941. Disponível https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 13 jun. 2025.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos. Brasília, DF: Presidência da República, 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 13 jun. 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. Brasília, DF: Presidência da República, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 13 jun. 2025.

BRASIL. Lei nº 14.155, de 27 de maio de 2021. Altera o Código Penal para agravar penas de crimes cibernéticos. Brasília, DF: Presidência da República, 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm. Acesso em: 13 jun. 2025.

BRASIL. Superior Tribunal de Justiça. Decisões sobre admissibilidade de provas digitais e proteção constitucional. 2018.

BRASIL. Superior Tribunal de Justiça. Resp 1.660.168/SP. Reconhece responsabilidade de provedores digitais em caso de conivência ou omissão. 2017.

BRASIL. Superior Tribunal de Justiça. STJ decide conflito de competência em caso de estelionato eletrônico. Brasília, 2022. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/30052022-Lei-14-5552021-so-alterou-competencia-para-julgamento-de-estelionato-em-casos-especificos.aspx. Acesso em: 7 ago. 2025.

BRASIL. Supremo Tribunal Federal. Decisões do ministro Alexandre de Moraes ampliando o alcance das investigações sobre crimes digitais relacionados a organizações criminosas e milícias digitais. 2025.

BRASIL. Supremo Tribunal Federal. Inquérito nº 4.781/DF. Decisão que reconhece a natureza permanente dos crimes virtuais. 2021.

BRASIL. Supremo Tribunal Federal. Recursos Extraordinários nº 1.037.396 e 1.057.258 - Tema 987 da Repercussão Geral. Responsabilidade das plataformas digitais. 2020.

CÂMARA DOS DEPUTADOS. Projeto de Lei sobre busca e apreensão em crimes cibernéticos. 2020. Disponível https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2236146. Acesso em: 13 jun. 2025.

CÂMARA DOS DEPUTADOS. Projeto de Lei sobre medidas cautelares em crimes cibernéticos. 2023. Disponível em: https://www.camara.leg.br/noticias/962444-ccj-aprova proibicao-de-acesso-a-internet-para-acusados-de-crimes-ciberneticos/. Acesso em: 13 jun. 2025.

CARVALHO, A. Competência da Polícia Federal em crimes transnacionais. Revista Jurídica, v. 10, n. 2, p. 45-60, 2022. Disponível em: https://www.scielo.br/. Acesso em: 13 jun. 2025.

CASELLI, R. Desafios na investigação de crimes cibernéticos. São Paulo: Editora Jurídica, 2022.

CISC GOV.BR. Centro Integrado de Segurança Cibernética. 2023. Disponível em: https://www.gov.br/cisc/pt-br. Acesso em: 13 jun. 2025.

CNN Brasil. WhatsApp continua alvo de clonagem e golpes digitais em São Paulo. CNN Brasil, 2025. Disponível em: https://www.cnnbrasil.com.br/tecnologia/whatsapp-em-2020/. Acesso em: 7 ago. 2025.

CNJ. Protocolos para preservação de provas digitais. Brasília: Conselho Nacional de Justiça, 2020. Disponível em: https://www.cnj.jus.br/. Acesso em: 13 jun. 2025.

COLE, D. Cybercrime and international cooperation. International Journal of Cyber

Criminology, v. 6, n. 1, p. 89-102, 2012. Disponível em: https://www.jstor.org/. Acesso em: 13 jun. 2025.

CONEXIS. Colaboração com provedores de internet no combate ao cibercrime. 2025. Disponível em: https://conexis.org.br/conexis-apresenta-as-prioridades-legislativas-do-setor de-telecomunicacoes/. Acesso em: 13 jun. 2025.

CONJUR. Impactos da atuação da ANPD nas investigações criminais. 2023. Disponível em: https://www.conjur.com.br/2023-mai-09/direito-digital-destaques-atuacao-anpd-2023-ano anterior/. Acesso em: 13 jun. 2025.

COUNCIL OF EUROPE. Convenção de Budapeste sobre Cibercrime. 2023. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/convencao-de-budapeste-e-promulgada-no-brasil. Acesso em: 13 jun. 2025.

DUQUE, M. Criptografia e investigação criminal. Rio de Janeiro: Lumen Juris, 2022.

ESMPU. Forças-tarefas no combate ao cibercrime. Brasília: Escola Superior do Ministério Público da União, 2024. Disponível em: https://www.mpm.mp.br/arquivos/67476. Acesso em: 13 jun. 2025.

FACHIN, L. Integração institucional no combate ao cibercrime. Revista do STF, v. 12, n. 3, p. 20-35, 2024. Disponível em: https://www.scielo.br/. Acesso em: 13 jun. 2025.

FBSP. Anuário Brasileiro de Segurança Pública 2023. São Paulo: Fórum Brasileiro de Segurança Pública, 2023. Disponível em: https://forumseguranca.org.br/. Acesso em: 13 jun. 2025.

FEBRABAN. *Golpe da falsa central telefônica: saiba como funciona e como se proteger*. São Paulo: Federação Brasileira de Bancos, 14 jun. 2024. Disponível em: https://portal.febraban.org.br/noticia/4137/pt-br/. Acesso em: 8 ago. 2025.

FEBRABAN. Relatório de Fraudes Digitais 2024. São Paulo: Federação Brasileira de Bancos, 2024. Disponível em: https://portal.febraban.org.br/. Acesso em: 13 jun. 2025.

FEBRABAN. Laboratórios de cibersegurança. 2024. Disponível em: https://febrabantech.febraban.org.br/temas/seguranca/laboratorio-de-seguranca-cibernetica-da-febraban-faz-3-anos-com-11-mil-participacoes. Acesso em: 13 jun. 2025.

FERREIRA, L. Falta de estrutura nas investigações cibernéticas. Revista de Segurança Pública, v. 15, n. 1, p. 30-45, 2022. Disponível em: https://www.scielo.br/. Acesso em: 13 jun. 2025.

FREITAS, R. Cooperação com empresas privadas no combate ao cibercrime. São Paulo: Saraiva, 2021.

FREITAS JUNIOR, P.; LYRA NETO, J. Obstáculos jurisdicionais em crimes cibernéticos. Revista Brasileira de Direito Penal, v. 9, n. 2, p. 55-70, 2022. Disponível em: https://www.scielo.br/. Acesso em: 13 jun. 2025.

FRANCO, P. Perícia forense digital. São Paulo: Saraiva, 2023.

FULLER, J. Medidas cautelares em crimes digitais. Journal of Cyber Law, v. 5, n. 3, p. 120 135, 2021. Disponível em: https://www.jstor.org/. Acesso em: 13 jun. 2025.

G1. Golpistas deram prejuízo de quase R$ 2 milhões após mais de 100 anúncios falsos de vendas de veículos em todo país, diz polícia. 22 fev. 2024. Disponível em: https://g1.globo.com/go/goias/noticia/2025/05/22/golpistas-deram-prejuizo-de-quase-r-2-milhoes-apos-mais-de-100-anuncios-falsos-de-vendas-de-veiculos-em-todo-pais-diz-policia.ghtml. Acesso em: 8 ago. 2025.

G1. MPRJ realiza operação contra quadrilha de hackers em Barra Mansa. Rio de Janeiro, 13 ago. 2019. Disponível em: https://g1.globo.com/rj/sul-do-rio-costa-verde/noticia/2019/08/13/mprj-realiza-operacao-contra-quadrilha-de-hackers-em-barra-mansa.ghtml. Acesso em: 8 ago. 2025.

IBGE. Pesquisa Nacional por Amostra de Domicílios Contínua: Tecnologia da Informação e Comunicação 2023. Rio de Janeiro: Instituto Brasileiro de Geografia e Estatística,

2023. Disponível em: https://www.ibge.gov.br/estatisticas/sociais/populacao/22827-pesquisa nacional-por-amostra-de-domicilios-continua-tecnologia-da-informacao-e-comunicacao.html. Acesso em: 13 jun. 2025.

INAC. Operação 404: Combate à pirataria digital. 2023. Disponível em: https://g1.globo.com/politica/noticia/2023/11/28/operacao-404-nova-fase-cumpre-mandados no-brasil-e-em-outros-paises.ghtml. Acesso em: 13 jun. 2025.

KERR, O. Digital Evidence and the Fourth Amendment. Harvard Law Review, v. 123, n. 4, p. 800-850, 2010. Disponível em: https://www.jstor.org/. Acesso em: 13 jun. 2025.

KROLL. Geolocalização em investigações digitais. 2025. Disponível em: https://www.kroll.com/pt-br/o-que-fazemos/seguranca-cibernetica/investigacao-e-resposta. Acesso em: 13 jun. 2025.

MENDES, R.; TORRES, L. Cooperação interinstitucional no combate ao cibercrime. Revista de Direito Penal, v. 8, n. 1, p. 90-110, 2020. Disponível em: https://www.scielo.br/. Acesso em: 13 jun. 2025.

MIGALHAS. Competência do Ministério Público em investigações criminais. 2025. Disponível em: https://www.migalhas.com.br/quentes/426827/stf-reafirma-competencia-concorrente-do-mp-em-investigacoes-criminais. Acesso em: 13 jun. 2025.

MJSP. Acordo Febraban-MJSP para combate a fraudes digitais. Ministério da Justiça e Segurança Pública, 2022. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/mjsp-e-febraban-firmam-acordo-para-combate-a-fraudes-golpes-e-crimes-ciberneticos. Acesso em: 13 jun. 2025.

MJSP. Convenção da ONU contra crimes cibernéticos. Ministério da Justiça e Segurança Pública, 2024. Disponível em: https://agenciagov.ebc.com.br/noticias/202408/onu-aprova-proposta-que-podera-reforcar-o-enfrentamento-a-crimes-ciberneticos. Acesso em: 13 jun. 2025.

MJSP. Aliança Nacional de Combate a Fraudes Digitais. Ministério da Justiça e

Segurança Pública, 2025. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/lewandowski-criminalidade-digital-e-alarmante-e-exige-resposta-inteligente. Acesso em: 13 jun. 2025.

MPBA. Integração multissetorial no combate ao cibercrime. Salvador: Ministério Público da Bahia, 2023. Disponível em: https://www.mpba.mp.br/noticia/48060. Acesso em: 13 jun. 2025.

MPDFT. Núcleo Especial de Combate aos Crimes Cibernéticos. Brasília: Ministério Público do Federal e Territórios, 2025. em: https://www.mpdft.mp.br/portal/index.php/conhecampdft-menu/nucleos-e-grupos/nucleo-de-combate-a-crimes-ciberneticos-ncyber. Acesso em: 13 jun. 2025.

MPF. Cooperação internacional em crimes cibernéticos. Brasília: Ministério Público Federal, 2023. Disponível em: https://www.mpf.mp.br/. Acesso em: 13 jun. 2025.

MPMG. Parcerias com universidades no combate ao cibercrime. Belo Horizonte: Ministério Público de Minas Gerais, 2023. Disponível em: https://www.mpmg.mp.br/portal/menu/areas de-atuacao/criminal/crimes-ciberneticos/. Acesso em: 13 jun. 2025.

MPPI. Desafios na investigação de crimes cibernéticos. Teresina: Ministério Público do Piauí, 2022. Disponível em: https://www.mppi.mp.br/internet/wp-content/uploads/2022/06/Crimes ciberneticos-e-investigacao-policial.pdf. Acesso em: 13 jun. 2025.

MPU. Procedimentos investigativos em crimes digitais. Brasília: Ministério Público da União, 2022. em: https://transparencia.mpf.mp.br/conteudo/atividade-fim/procedimentos-investigatorios. Acesso em: 13 jun. 2025.

MRE. Força-Tarefa contra Ransomware no Brasil. Ministério das Relações Exteriores, 2025. Disponível em: https://www.gov.br/mre/pt-br/acesso-a-informacao/consultas-publicas/forca tarefa-contra-o-ransomware-no-brasil-rtf-brasil-1. Acesso em: 13 jun. 2025.

NIST. Guidelines on Mobile Device Forensics. National Institute of Standards and Technology, 2020. Disponível em: https://www.nist.gov/. Acesso em: 13 jun. 2025.

NORTON. Cyber Security Insights Report 2022. Norton, 2022. Disponível em: https://www.nortonlifelock.com/about/newsroom/cyber-safety-insights-report. Acesso em: 13 jun. 2025.

NORTONLIFELOCK. 2022 Norton Cyber Safety Insights Report: Home & Family. Mountain View, NortonLifeLock Inc., 2022. Disponível em: https://www.nortonlifelock.com/about/newsroom/cyber-safety-insights-report. Acesso em: 13 jun. 2025.

O GLOBO. ANPD intensifica fiscalização de vazamentos de dados. Rio de Janeiro, 2024. Disponível https://oglobo.globo.com/economia/noticia/2024/10/25/em-um-mes autoridade-brasileira-de-dados-abre-mais-investigacoes-contra-empresas-do-que-em-quatro anos.ghtml. Acesso em: 13 jun. 2025.

PC-AM. Delegacia de Repressão a Crimes Cibernéticos. Manaus: Polícia Civil do Amazonas, 2024. Disponível em: https://www.ssp.am.gov.br/crimes-ciberneticos-policia-civil-detalha crimes-mais-comuns-e-orienta-sobre-como-denuncia-los/. Acesso em: 13 jun. 2025.

POLÍCIA CIVIL DO ESTADO DE GOIÁS. Operação desarticula grupo que aplicava golpes com anúncios falsos de veículos no OLX, causando prejuízos superiores a R$ 2 milhões. Goiânia, 2021. Disponível em: https://www.policiacivil.go.gov.br/tag/golpe-olx/. Acesso em: 7 ago. 2025.

POLÍCIA FEDERAL. Forças-tarefas no combate ao cibercrime. Brasília: Polícia Federal, 2022. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/policia-federal-cria-unidade-especial-para-intensificar-a-repressao-a-crimes-ciberneticos. Acesso em: 13 jun. 2025.

POLÍCIA FEDERAL. Operação contra organização criminosa que desviou valores de mais de 200 contas bancárias e converteu recursos em criptomoedas para o exterior. Brasília, 2023. Disponível em: https://www.cnnbrasil.com.br/nacional/operacao-contra-criptomoedas-

bloqueia-r-9-bilhoes-de-investigados/#goog_rewarded. Acesso em: 7 ago. 2025.

POLÍCIA FEDERAL. Unidade Especial de Investigação de Crimes Cibernéticos. Brasília: Polícia 2023. Disponível em: https://www.gov.br/pf/pt-br/assuntos/noticias/2022/06/pf-lanca-unidade-especial-para-reprimir-crimes-ciberneticos. Acesso em: 13 jun. 2025.

ROCHA, T. Convenção de Budapeste e o Brasil. Revista de Direito Internacional, v. 10, n. 1, p. 78-95, 2023. Disponível em: https://www.scielo.br/. Acesso em: 13 jun. 2025.

SANTA CATARINA. Polícia Civil. Polícia Civil deflagra Operação BitTrack para desarticular organização criminosa especializada em fraudes bancárias. Florianópolis, 10 out. 2024. Disponível em: https://pc.sc.gov.br/?p=24119. Acesso em: 8 ago. 2025.

SANTOS, J. Estratégias para o combate ao cibercrime. São Paulo: Atlas, 2024.

SERPRO. Aliança Nacional de Combate a Fraudes Digitais. 2025. Disponível em: https://www.serpro.gov.br/menu/noticias/noticias-2025/serpro-integra-alianca-nacional-combate-fraudes-digitais. Acesso em: 13 jun. 2025.

SDS. Capacitação em crimes cibernéticos. Recife: Secretaria de Defesa Social, 2024. Disponível em: https://www.sds.pe.gov.br/noticias/11268-sds-lanca-cartilha-digital-com-orientacoes-de-prevencao-contra-os-crimes-virtuais. Acesso em: 13 jun. 2025.

SILVA, M.; OLIVEIRA, T. Deep Web e crimes cibernéticos. Revista de Tecnologia e Direito, v. 7, n. 2, p. 65-80, 2021. Disponível em: https://www.scielo.br/. Acesso em: 13 jun. 2025.

SSP-SP. Investigação de apologia à violência digital. São Paulo: Secretaria de Segurança Pública, Disponível em: https://www.agenciasp.sp.gov.br/violencia-digital investigacao-noad/. Acesso em: 13 jun. 2025.

STJ. Conflitos de competência em crimes cibernéticos. Brasília: Superior Tribunal de Justiça, 2022. Disponível em: https://www.stj.jus.br/. Acesso em: 13 jun. 2025.

TJPB. Busca e apreensão em crimes cibernéticos. João Pessoa: Tribunal de Justiça da Paraíba, 2024. Disponível em: https://www.tjpb.jus.br/noticia/justica-determina-busca-e-apreensao-de-equipamentos-de-acusado-de-crimes-ciberneticos. Acesso em: 13 jun. 2025.

TREND MICRO. Ferramentas forenses digitais. 2024. Disponível em: https://www.trendmicro.com/pt_br/business.html. Acesso em: 13 jun. 2025.

UFPEL. Parcerias acadêmicas no combate ao cibercrime. Pelotas: Universidade Federal de Pelotas, 2024. Disponível em: https://www.ufpel.edu.br/. Acesso em: 13 jun. 2025.

WALL, D. Cybercrime: The transformation of crime in the information age. Cambridge: Polity Press, 2007.

WENDT, C. Técnicas de investigação em crimes virtuais. Revista de Segurança Digital, v. 5, n. 1, p. 22-38, 2024. Disponível em: https://www.scielo.br/. Acesso em: 13 jun. 2025.