v. 15, n. 1, p. 13-23, 2026
ISSN 2237-9223

REVISTA BRASILEIRA DE CRIMINALÍSTICA

DOI: http://dx.doi.org/10.15260/rbc.v15i1.955

Combate ao Estelionato Eletrônico no Brasil: análise das condições de investigação ocorridas no Pará, Piauí, Distrito Federal, São Paulo e Paraná

A.P.C. Oliveira [a,*], D.A. Gomes [a,*]

[a] *Universidade Federal do Sul e Sudeste do Pará - UNIFESSPA*

**Endereço de e-mail para correspondência: ana.oliveira@unifesspa.edu.br / diagomes@unifesspa.edu.br*

Recebido em 12/03/2025; Revisado em 25/10/2025; Aceito em 09/12/2025

Resumo

O presente trabalho buscou investigar as condições de combate ao estelionato eletrônico no Brasil com foco em alguns estados representando as cinco regiões, Pará (Norte), Piauí (Nordeste), Distrito Federal (Centro-Oeste), São Paulo (Sudeste) e Paraná (Sul). A pesquisa, de abordagem qualitativa e exploratória, baseou-se em fontes documentais e bibliográficas. Para a análise comparativa, foram considerados os aspectos como data de criação, estrutura administrativa, recursos, metodologia de investigação, parcerias, capacitação de agentes e estrutura de recebimento de denúncias. Os resultados mostram diferentes graus de maturidades das instituições analisadas, sendo refletidas nas políticas públicas adotadas por cada estado no enfrentamento ao estelionato eletrônico. Conclui-se através desse estudo que há necessidade de criação de um sistema integrado para o combate aos crimes cibernéticos, além de uma atuação mais efetiva na conscientização da população através de campanhas educativas. E por fim, é destacada a importância de políticas públicas voltadas para a modernização tecnológica e formação contínua dos agentes no combate a esse tipo de crime.

Palavras-Chave: Estelionato Eletrônico; Crimes Cibernéticos; Investigação; Políticas Públicas.

Abstract

The present study sought to investigate the conditions for combating electronic fraud in Brazil, focusing on states representing the five regions: Pará (North), Piauí (Northeast), Federal District (Central-West), São Paulo (Southeast), and Paraná (South). The research, with a qualitative and exploratory approach, was based on documentary and bibliographic sources. For the comparative analysis, aspects such as creation date, administrative structure, resources, investigation methodology, partnerships, agent training, and complaint-receiving structures were considered. The results reveal varying levels of institutional maturity among the analyzed states, reflected in the public policies adopted to address electronic fraud. The study concludes that there is a need to establish an integrated system to combat cybercrimes and to implement more effective public awareness campaigns through educational initiatives. Lastly, the importance of public policies focused on technological modernization and the continuous training of agents to combat this type of crime is emphasized.

Keywords: Eletronic Fraud; Cybercrimes; Investigation; Public Policies.

1. INTRODUÇÃO

Nas últimas décadas, a internet desempenhou um papel importante na transformação social e econômica do Brasil, permitindo maior conectividade, melhoria na acessibilidade de informação e o crescimento no comércio eletrônico. Porém, a crescente utilização da rede também trouxe desafios, principalmente no que se refere à segurança digital [1].

A designação crime cibernético ainda não é uniforme dentre os doutrinadores no campo jurídico, podendo essa nomenclatura possuir variações como crimes digitais, crimes virtuais ou crimes de informática [2].

De acordo com [3], crimes de informática são tipificados no Direito Penal como sendo realizado através de computadores ou que tem como alvo computadores, sistemas informáticos, ou os dados e informações que neles são processados ou armazenados.

[4] Conceitua crime virtual como uma conduta típica, ilícita e culpável, ocorrida com dolo ou culpa. Tal ação pode ser realizada por indivíduos ou organizações, utilizando-se de recursos informáticos, tanto na internet quanto fora dela, violando a segurança dos sistemas informáticos.

Já [5], conceitua o crime cibernético em duas vertentes: ataques sofisticados e crimes habilitados por tecnologia. No primeiro, o crime é praticado por meio da utilização de tecnologias avançadas e métodos complexos, exemplificando com o *hacking*, *malware* e extorsão DDoS, enquanto no segundo, são caracterizados por crimes tradicionais que através da tecnologia o fazem para realizar roubos, fraudes online e ciberterrorismo.

No Brasil, dentre os diversos crimes cibernéticos que tem aumentado, destaca-se o estelionato eletrônico, no qual visa enganar as vítimas para obter uma vantagem financeira ou roubar informações confidenciais. Segundo [6], empresa referência em inteligência de dados e soluções antifraude, no Mapa da fraude em 2023, o Brasil registrou mais de 3 milhões de tentativas de fraude online, permanecendo ainda o Brasil nas primeiras posições em ocorrências de crimes digitais no mundo.

Dentre os tipos de crimes cibernéticos praticados, o estelionato eletrônico no Brasil pode ocorrer por diversas maneiras, desde o *phishing* até golpes de falso suporte técnico e pirâmides financeiras. Esse aumento está diretamente relacionado à maior inclusão digital da população e à expansão do comércio eletrônico que atingiu um volume recorde durante a pandemia da Covid-19. Ao mesmo tempo, o déficit na segurança de informação, combinada com a falta de conscientização por parte dos usuários, contribuiu para a vulnerabilidade do ambiente online, facilitando a ação de criminosos virtuais [7].

O combate ao crime cibernético exige um aperfeiçoamento tecnológico na esfera policial e judicial. É necessário que as polícias trabalhem principalmente desenvolvendo suas próprias tecnologias adaptadas para solucionar esses tipos de crimes. Essas tecnologias precisam ser utilizadas de forma cooperativa para que as polícias dos estados trabalhem em conjunto no combate a esse delito [2].

Diante desse cenário, o objetivo geral deste artigo é analisar as condições de investigação no combate ao crime de estelionato eletrônico nos estados do Pará, Piauí, Distrito Federal, São Paulo e Paraná. Para os objetivos específicos buscamos analisar a estrutura e atuação dessas instituições no combate aos crimes eletrônicos e identificar as ações de conscientização e prevenção que as polícias civis dos estados selecionados fazem junto a sociedade a fim de minimizar o número de ocorrências desse tipo de crime.

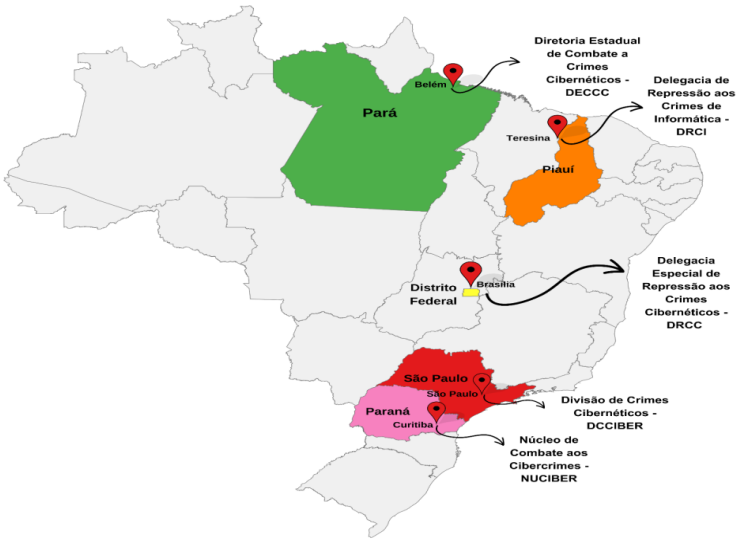

Figura 1: Mapa com os estados brasileiros analisados

2. METODOLOGIA

2.1. Objeto de Estudo

A pesquisa seguiu uma abordagem qualitativa de caráter exploratório, pois é o mais adequado para compreender de forma mais aprofundada as ações e estratégias adotadas pelas autoridades brasileiras no enfrentamento ao estelionato eletrônico. A opção pela abordagem qualitativa fundamenta-se no pressuposto de que conforme [8], a realidade social é complexa, dinâmica e construída a partir das interpretações e significados atribuídos pelos sujeitos e pelas instituições envolvidas. Nesse sentido, [9] afirmam que esse tipo de pesquisa busca uma análise detalhada das interações e dos processos, priorizando a interpretação dos comportamentos e das práticas humanas dentro de um determinado contexto social.

Dessa forma, o objetivo principal foi identificar, a partir das fontes bibliográficas e documentais, as medidas adotadas pelas autoridades brasileiras para enfrentar esse tipo de crime, que tem aumentado com a popularização da internet. O ponto de partida foi a definição do problema, o qual consiste em analisar de modo comparativo as condições de investigação de combate ao estelionato eletrônico ocorridas no cenário nacional.

Para tanto, foram escolhidos os seguintes estados: Pará, Distrito Federal, São Paulo, Piauí e Paraná. O Pará foi incluído por situar-se na região norte onde há desafios relacionados à infraestrutura tecnológica e logística. O Distrito Federal foi selecionado por concentrar órgãos federais de investigação e possuir elevados investimentos em tecnologia e capacitação de pessoal e que também devido a concentração de órgãos políticos, serve como parâmetro de comparação nacional. O estado de São Paulo, maior centro econômico do país, apresenta um elevado número absoluto de registros de crimes cibernéticos, refletindo desafios da gestão pública nas investigações em um ambiente altamente digitalizado. O Piauí, representante da região nordeste, foi selecionado pelo aumento da criminalidade cibernética nesse estado e pela modernização que a polícia civil piauiense tem passado e assim se destacado no combate a esses crimes. E por fim, o Paraná foi escolhido como representante da região Sul por apresentar experiências já consolidadas e devido a ser o primeiro estado a instituir uma área especializada em investigação de crimes cibernéticos.

A Figura 1 mostra os estados escolhidos e suas respectivas instituições. No estado do Pará, o órgão responsável pela investigação desse tipo de crime é a Polícia Civil, através da Diretoria Estadual de Combate a Crimes Cibernéticos (DECC); no Distrito Federal através da Delegacia Especial de Repressão aos Crimes Cibernéticos (DRCC); no estado de São Paulo, dentro da Polícia Civil, através da Divisão de Crimes Cibernéticos (DCCIBER); no Piauí, através da Delegacia de Repressão aos Crimes de Informática (DRCI); e no estado do Paraná, através no Núcleo de Combate ao Cibercrimes (Nuciber) que se encontra dentro da Polícia Civil do estado do Paraná.

2.2. Coleta de Dados

A coleta de dados foi realizada por meio de pesquisa bibliográfica e documental, utilizando como fontes artigos acadêmicos, legislações vigentes, publicações de órgãos governamentais e não governamentais, além de relatórios disponíveis na internet. Para a pesquisa bibliográfica foram consultados artigos e dissertações disponíveis em base de dados eletrônicas como Scielo, Google Acadêmico e Capes, com a utilização dos *strings* de busca “crimes virtuais”, “estelionato eletrônico”, “crime cibernético”, “investigação policial”. Para a pesquisa documental foram utilizadas leis, decretos, relatórios governamentais e publicações oficiais de órgãos como Ministério da Justiça e Segurança Pública, Polícia Civil dos estados.

Após a coleta, os materiais foram analisados sendo selecionados aqueles que apresentavam maior relevância e adequação aos objetivos propostos pela pesquisa e priorizando os conteúdos publicados nos últimos 5 anos.

2.3. Metodologia de Análise

A análise dos dados coletados foi realizada através da análise descritiva, que tem como objetivo a observação, registro e interpretação dos fenômenos, buscando compreender suas características, padrões e relações sem a intenção de interferir neles. Segundo [10], a análise descritiva visa descrever com precisão os fatos e as relações existentes em determinado fenômeno, permitindo uma visão ampla e sistematizada da realidade estudada.

Na pesquisa abordada e conforme [9], buscou-se identificar padrões, tendências e desafios recorrentes nas estratégias de combate ao estelionato eletrônico nas práticas de investigação das autoridades policiais e nos mecanismos preventivos adotados pelas instituições financeiras e empresas de tecnologia.

O tratamento dos dados coletados foi feito através de uma leitura crítica e sistematizada das informações para identificar tendências, padrões e desafios enfrentados na investigação nos crimes de estelionato eletrônico. Esses dados foram utilizados para elaboração de um quadro comparativo, no qual foram analisados os seguintes aspectos: histórico de criação que se refere a data e o contexto em que os departamentos

e/ou divisões especializadas no combate ao crime cibernético foram criados; a estrutura administrativa que visa a organização interna destes departamentos e/ou divisões, bem como a quantidade de servidores efetivo nas polícias civis dos estados selecionados; a competência dos agentes envolvidos nesse tipo de operação, ou seja, o nível de especialização dos policiais; parcerias com outras instituições; recursos destinados através da Lei de Orçamento Anual de cada estado ao combate ao estelionato eletrônico; a metodologia de investigação, ou seja, os métodos e as tecnologias usadas para investigar essa modalidade de crime e a estrutura de recebimento de denúncias.

Também foi realizada uma análise referente a dados obtidos através do [15] concernente à evolução dos registros desse tipo de crime nos estados selecionados.

Todas essas informações foram consolidadas de forma a fazer um diagnóstico entre as regiões do Brasil e verificar o grau de maturidade de cada instituição, além de apresentar tendências e lacunas nas políticas de combate aos crimes cibernéticos.

3. RESULTADOS E DISCUSSÃO

De acordo com os dados apresentados na Tabela 1, referente a atuação das polícias civis dos estados do Pará, Piauí, São Paulo, Distrito Federal e Paraná para o combate aos crimes virtuais, nota-se um cenário variado em relação à estrutura administrativa, quantidade de servidores efetivos, recursos disponíveis e a metodologia de investigação. Quanto aos demais aspectos encontramos algumas semelhanças no qual serão detalhadamente descritos. Cada estado desenvolveu uma abordagem específica para o enfrentamento dos crimes virtuais, adequando sua prática com os recursos tecnológico, humano e financeiro disponíveis e parcerias com demais instituições para melhorar a eficiência na investigação desse tipo de crime.

Tabela 1: Comp**arativo estrutural das Polícias Civis no combate ao crime Cibernético**

	PC-PA	**PC-DF**	**PC-SP**	**PC-PI**	**PC-PR**
Criação	16/04/2020 [11]	31/03/2017 [19]	13/10/2020 [25]	Início/2017 [32]	18/11/2005 [38]
Estrutura Administrativa	Diretoria Estadual de Combate a Crimes Cibernéticos (DECCC) [12]	Delegacia Especial de Repressão aos Crimes Cibernéticos (DRCC) [20]	Divisão de Crimes Cibernéticos (DCCIBER) [25]	Delegacia de Repressão aos Crimes de Informática (DRCI) [32]	Núcleo de Combate aos Cibercrimes (Nuciber) [38]
Servidores Ativos	3.758 [13]	4.487 [21]	27.135 [26]	N.I	4.130 [39]
Competência dos Agentes	Cursos frequentes de aperfeiçoamento em crimes virtuais [11]	Cursos frequentes de aperfeiçoamento em crimes virtuais [22]	Cursos frequentes de aperfeiçoamento em crimes virtuais [27]	Cursos frequentes de aperfeiçoamento em crimes virtuais [33]	Cursos frequentes de aperfeiçoamento em crimes virtuais [40]
Parcerias	PF e Polícia Civis estaduais [14]	PF e Polícia Civis estaduais [23]	PF e Polícia Civis estaduais [28]	PF e Polícia Civis estaduais e MP [34]	SAFERNET [41]
Nº registro de Estelionato Eletrônico	4.226 [15]	18.199 [15]	N.I.* [15]	888 [15]	8.749 [15]
Orçamento (100 mil hab)	12,66 [16]	6,11 [21]	13,04 [29]	0,22 [35]	6,42 [42]
Metodologia de Investigação	Sistema Guardião para varredura de dispositivos [17]	N.I	Software Cellebrite e outras ferramentas de análise [30]	Ferramentas de rastreamento e análise digital [36]	Ferramentas de rastreamento e análise digital [43]
Recebimento de Denúncias	BO presencial ou pela Delegacia virtual [18]	BO na Delegacia Eletrônica, e-mail e pelo WhatsApp [24]	BO na Delegacia Eletrônica [31]	BO presencial ou Delegacia virtual [37]	BO na Delegacia Eletrônica [43]

Fonte: autor, 2025

3.1. Criação

A criação de departamentos e delegacias especializadas no combate aos crimes virtuais são relativamente novos, o que demonstra um processo gradual e desigual das instituições de segurança pública no enfrentamento a esse tipo de crime.

O pioneirismo do Paraná em 2005 com a criação do Núcleo de Combate aos Cibercrimes (Nuciber), que apesar de ser um marco inicial importante, não difundiu o mesmo processo para outros estados. Isso sugere que o pioneirismo na criação de estruturas especializadas, não garante o amadurecimento institucional, principalmente quando há ausência de planejamento nacional coordenado para o enfrentamento aos crimes cibernéticos.

Pode ser observado ainda que essa diferença temporal de criação dos órgãos especializados nos estados selecionados, sendo o primeiro pelo Nuciber (2005) e as mais recentes, a Diretoria Estadual de Combate a Crimes Cibernéticos (DECCC) no estado do Pará (2020), e a Divisão de Crimes Cibernéticos (DCCIBER) no estado de São Paulo (2020), indica um modelo reativo e não preventivo no combate aos crimes cibernéticos.

Esse fato pode ser comprovado devido a criação desses órgãos terem sido efetivados durante ou logo após o período pandêmico o que força uma resposta emergencial e não um amadurecimento de estratégias para o combate a esses crimes.

3.2. Estrutura Administrativa

A estrutura administrativa das Polícias Civis analisadas se diferem bastante em sua organização para o combate aos crimes virtuais.

No Pará, a estrutura administrativa está sob a responsabilidade da Diretoria Estadual de Combate a Crimes Cibernéticos (DECCC), com atribuição de prevenção e repreensão das ações delituosas de natureza penal cometidas por meio tecnológicos que utilizam computadores, redes digitais, dispositivo de comunicação ou qualquer outro sistema informatizado. Essa diretoria desdobra-se em três divisões, cada uma atuando em uma frente de investigação, sendo crimes contra direitos individuais, crimes econômicos e patrimoniais e crimes contra grupos vulneráveis, todos perpetrados através dos meios virtuais. Essa segmentação interna demonstra um esforço recente de institucionalização e especialização das investigações, mas ainda necessita de indicadores sobre sua efetividade operacional.

No Distrito Federal, foi criada de forma especializada a Delegacia Especial de Repressão aos Crimes Cibernéticos (DRCC), que conduz investigações de alta complexidade de delitos graves cometidos pela internet. A centralização das investigações em uma unidade especializada reflete a capacidade técnica e o nível de investimento tecnológico, servindo como referência para outras polícias civis estaduais.

Já em São Paulo, a organização é por meio da Divisão de Crimes Cibernéticos (DCCIBER) que está vinculada ao Departamento Estadual de Investigações Criminais (DEIC). A DCCIBER tem por atribuição apurar fraudes praticadas por meio eletrônico, com envolvimento de organizações criminosas ou com o emprego de recursos de alta tecnologia. São vinculadas ao DCCIBER, quatro delegacias especializadas: Fraude contra instituições financeiras praticadas por meio eletrônico, fraudes contra instituição de comércio eletrônico praticados por meio eletrônico, violação de dispositivos eletrônicos e Redes de Dados e lavagem e ocultação de ativos ilícitos praticados por meio eletrônico. Esse nível de subdivisão evidencia um estágio avançado de maturidade institucional no combate aos crimes virtuais.

No Piauí, o combate aos crimes virtuais é feito por meio da Delegacia de Repressão aos Crimes de Informática (DRCI), com atribuição para investigar todos os crimes praticados através da internet.

No Paraná, apesar de ser a estrutura mais antiga existente, ela é denominada como um núcleo, ou seja, não trata-se de um departamento ou delegacia, o Núcleo de Combate aos Cibercrimes realiza a investigação de infrações penais cometidas com o uso ou emprego de meios ou recursos tecnológicos de informação computadorizada, esse núcleo também presta auxílio aos demais órgãos da Polícia Civil.

Apesar das estruturas específicas para a investigação de crimes cibernéticos, o efetivo das corporações está com um quadro de servidores bem aquém do quantitativo necessário, sendo que os números apresentados na Tabela 1 referem-se ao total geral, não sendo feita aqui um desmembramento do número de agentes alocados para a investigação de crimes virtuais, pois essas informações não foram fornecidas em publicações oficiais.

Nota-se que dos dados obtidos, o Pará possui um contingente menor de agentes, podendo indicar uma limitação operacional no enfrentamento ao crime de estelionato eletrônico, em contrapartida, essa lacuna pode ser refletida no aumento no número de registros no ano de 2024.

3.3. Competência dos Agentes

Nesse aspecto, podemos observar que a competência dos agentes dos estados analisados se forma a partir do momento em que estes ingressam na corporação. Não é requerido desses agentes formação específica como condição para ingresso, porém durante toda a carreira estes agentes passam por frequentes cursos de aperfeiçoamento em crimes virtuais.

De maneira geral, os agentes recebem formação em áreas como segurança digital, análise forense e

técnicas de investigação aplicadas a crimes virtuais, pois esses crimes demandam abordagens diferentes das utilizadas para os delitos convencionais.

Ressalte-se que embora algumas instituições apresentem dados gerais sobre suas atividades, o detalhamento de carga horária, periodicidade e conteúdo, podem não ter todos os dados publicados pelas instituições, sendo apontado apenas em seus relatórios de gestão dados genéricos da capacitação de seus agentes.

3.4. Parcerias com outras instituições

As parcerias que ocorrem entre as polícias civis dos estados e outras instituições são empregadas de forma estratégica no combate aos crimes virtuais, uma vez que, esses crimes frequentemente envolvem redes complexas e jurisdições múltiplas. Essas parcerias proporcionam acesso a recursos especializados e fortalecem a capacidade investigativa dessas corporações.

Apesar da Polícia Federal (PF) possuir em sua competência a investigação de crimes cuja jurisdição seja federal, os crimes praticados por meio da rede mundial de computadores passam também pela sua competência. Porém, a PF atua em cooperação com as polícias civis dos estados, fornecendo recursos tecnológicos e operacionais para a atividade investigativa.

As Polícias Civis do Pará, Distrito Federal e São Paulo fazem suas investigações de crimes virtuais por meio de parcerias estratégicas com a Polícia Federal (PF), que proporciona tecnologia avançada e suporte técnico.

No Piauí, a Polícia Civil tem uma importante parceria com o Ministério Público estadual, facilitando ações legais e investigações que exigem intervenções rápidas, como o bloqueio de contas fraudulentas e a remoção de conteúdo online. Essa cooperação é crucial, pois o MP pode fornecer autorizações judiciais de maneira ágil, acelerando o processo investigativo e fortalecendo as ações de repressão a crimes cibernéticos no estado.

A Polícia Civil do Paraná se destaca por sua colaboração com a SAFERNET, uma organização de referência no enfrentamento de crimes e violações de direitos humanos na internet, incluindo casos de exploração infantil. Essa parceria possibilita o uso de recursos especializados em monitoramento digital e apoio técnico, ampliando a capacidade da Polícia Civil do Paraná para identificar e desmontar redes criminosas que operam no ambiente virtual.

3.5. Recursos Destinados

Os recursos destinados às instituições analisadas refere-se ao que consta na Lei Orçamentária Anual (LOA) do ano de 2024 para as respectivas polícias civis, considerado o orçamento/100 mil hab. Observa-se uma diferença significativa dos recursos recebidos em cada órgão, o que permite discutir possíveis relações entre o orçamento destinado e a capacidade de resposta e eficiência das polícias civis analisadas.

Entre os estados analisados, o Distrito Federal possui o maior número de registros de estelionato eletrônico em 2024 (18.199), mesmo possuindo um orçamento de 6,11 milhões por 100 mil hab. Esses registros poderiam indicar uma limitação no combate ao crime de estelionato eletrônico, porém cabe pontuar o contexto atual do DF.

O DF apresenta níveis de conectividade domiciliar entre os mais elevados do país, acima de 90%, conforme divulgado pelo Instituto Brasileiro de Geografia e estatística (2023) e que conforme o Instituto de Pesquisa Aplicada (2024) o DF tem a maior renda per capita do Brasil, e finalmente a polícia civil do DF possui seu sistema de registro totalmente digitalizado. Esses fatores contribuem para maior capacidade de notificação e resposta institucional, o que pode explicar o elevado número de casos registrados e não necessariamente a ineficácia do orçamento para esse órgão.

O Pará, com o segundo maior investimento (4.226), demonstra que o aumento do orçamento ainda não se traduz em evidências de redução significativa das ocorrências, o que sugere que os efeitos orçamentários dependem também da eficiência administrativa.

O Paraná (8.749) possui um investimento de um nível intermediário em comparação aos demais estados (6,42 mil/100 hab), por isso mostra um indicativo de estagnação, apresentando um alto volume de registros mesmo sendo o primeiro estado a instituir um órgão específico para esses tipos de crimes.

O Piauí (888), possui o menor investimento proporcional, podendo ser destacado talvez por subnotificações para esse registro devido a limitação da capacidade de registro. Já São Paulo, com o maior valor autorizado no orçamento, não informou o número de registros de estelionato eletrônicos para o ano de 2024.

3.6. Metodologia de Investigação

A metodologia de investigação para os crimes virtuais adotadas pelas Polícias Civis partem de variadas práticas com o objetivo de promover celeridade e assertividade na investigação, independente do método adotado.

No estado do Pará, a Diretoria Estadual de Combate a Crimes Cibernéticos (DECCC) utiliza o sistema Guardião, desenvolvido para monitoramento e varredura de dispositivos. Essa ferramenta permite vigilância em tempo real, essencial para rastrear atividades criminosas online de modo contínuo. No Distrito Federal, não foi possível encontrarmos registros de como a investigação é realizada.

A Polícia Civil de São Paulo, por sua vez, se destaca pelo uso do software *Cellebrite* e de outras ferramentas de análise digital na Divisão de Crimes Cibernéticos (DCCIBER). O *Cellebrite* é conhecido por sua precisão na extração de dados de dispositivos móveis, sendo essencial para investigações que requerem a recuperação de informações detalhadas, como mensagens e registros de chamadas, comumente utilizadas em casos de fraudes e extorsão digital.

No Piauí e no Paraná, as polícias civis também aplicam ferramentas de rastreamento e análise de dispositivos digitais, porém não especificadas de forma clara na pesquisa realizada.

3.7. Recebimento de Denúncias

O recebimento de denúncias de crimes virtuais nas Polícias Civis apresenta elementos similares que buscam facilitar o acesso da sociedade aos serviços de segurança, melhorando o fluxo de informações para investigações rápidas e eficientes.

Observa-se que a maioria dos estados pesquisados utiliza plataformas digitais para o registro de boletins de ocorrência, o que é um reflexo da necessidade de adaptar os canais de atendimento ao crescimento do ambiente virtual. As Polícias Civis do Pará, São Paulo e Paraná possuem em sua estrutura delegacias eletrônicas para o registro de ocorrências, o que permite ao cidadão denunciar crimes online sem precisar se deslocar a uma delegacia física.

Além das delegacias eletrônicas, algumas polícias também ampliam o leque de canais de atendimento para incluir outras formas de comunicação digital. A Polícia Civil do Distrito Federal, por exemplo, oferece o registro de denúncias não apenas pela Delegacia Eletrônica, mas também via e-mail e WhatsApp, diversificando as formas de contato com o público e garantindo que as informações cheguem rapidamente aos investigadores.

As Polícias Civis do Piauí e do Pará, mantêm tanto as delegacias físicas quanto as virtuais para o recebimento de denúncias, permitindo que pessoas sem acesso a dispositivos digitais ou internet possam denunciar crimes de maneira tradicional. Essa abordagem híbrida é particularmente importante em regiões onde o acesso à tecnologia ainda é limitado, garantindo que a população em geral possa colaborar com a polícia e fornecer informações relevantes para a resolução de crimes.

3.8. Registros de Estelionato Eletrônico

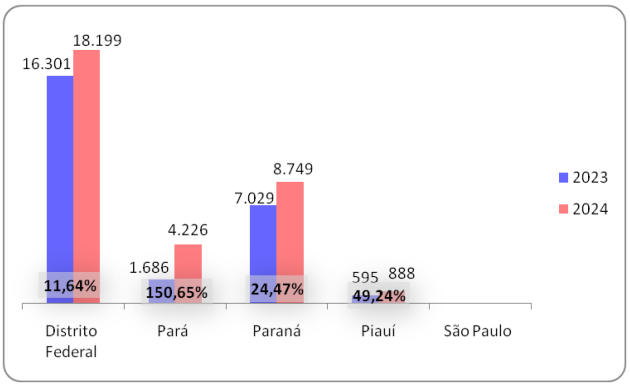

Figura 2: Estelionato por meio Eletrônico

Fonte: Autores, adaptado do Anuário Brasileiro de Segurança Pública (2025)

*Informação não disponível

Os dados retirados do Anuário Brasileiro de Segurança Pública (2025) referente ao aumento do crime de estelionato eletrônico comprovam a necessidade de uma rápida melhoria da estrutura da segurança pública. Conforme apresentado na Figura 2, esses números evoluíram rapidamente entre os anos de 2023 e 2024.

No Pará, houve um crescimento de 150%, e no Piauí, um aumento de 49,24%. O Distrito Federal também apresentou aumento, porém de forma mais moderada em relação aos demais estados, de 11,64%. No Paraná houve um aumento de 24,47%. Esses dados refletem uma tendência geral de crescimento do crime eletrônico.

Os dados apresentados na Tabela 1 nos mostram que as polícias têm buscado aperfeiçoamento através de cursos de capacitação para investigações nos crimes eletrônicos, assim como possuem uma estrutura semelhante quanto ao recebimento de denúncias desse tipo de crime, porém os investimentos nessas instituições acontecem de maneira bem diferenciada em cada órgão, podendo isso resultar em maior ou menor eficácia na contenção dos crimes eletrônicos, em especial o estelionato.

A maior variação no aumento de crimes de estelionato eletrônico de 2023 para 2024 ocorreu no estado do Pará, que apesar de possuir um orçamento relativamente alto na polícia civil ainda não há reflexos na redução do crime de estelionato eletrônico nesse estado.

Com a segunda maior variação, temos o estado do Piauí, que mesmo apresentando uma estrutura moderna e ter passado por uma reestruturação em 2023 [44], os investimentos nessa instituição podem ainda não serem

insuficientes para que a investigação nesse tipo de crime traga resultados melhores, daí resulta este aumento alarmante.

O Paraná, ocupando a terceira posição no aumento da variação do crime de estelionato eletrônico, apesar de apresentar um investimento razoável [45], ainda não conseguiu reduzir e/ou controlar esse crime, podendo indicar uma certa ineficácia nos meios empregados para prevenção e resolução desse delito.

Já no Distrito Federal, podemos ver uma variação controlada no aumento do estelionato eletrônico, sendo 11,64% de aumento em relação ao ano de 2023. Esse estado tem investido bastante na segurança pública, indicando uma assertividade dos métodos empregados tanto na prevenção quanto nas investigações.

Para o Anuário Brasileiro de Segurança Pública, São Paulo não disponibilizou os dados, porém segundo informações [46], São Paulo registrou um aumento de 6,6% nos crimes de estelionatos em 2024 comparado ao ano de 2023. Cabe ressaltar, que esses números se referem ao estelionato no geral, não havendo uma separação entre o estelionato tradicional e o eletrônico.

4. AÇÕES DE CONSCIENTIZAÇÃO DOS ESTADOS NA PREVENÇÃO DO ESTELIONATO ELETRÔNICO

Devido ao aumento dos crimes de estelionato eletrônico nos estados analisados apresentado no Gráfico 1, verificamos que a adoção de medidas de conscientização e prevenção voltadas para a proteção da população se torna extremamente necessária nesse cenário. Para [47] governos e empresas devem investir em campanhas educativas de navegação segura e conscientização sobre o bom uso da tecnologia. Diante disso, foram elencados algumas medidas que estão sendo adotadas por esses estados a fim de mitigar o crescimento desse delito.

No estado do Pará, o governo estadual sancionou em 2024 uma importante lei que institui a Campanha de Combate aos Crimes Cibernéticos Financeiros, com a promoção de campanhas durante o mês de setembro e tem como objetivos principais proteger potenciais vítimas, conscientizar a sociedade e incentivar o enfrentamento aos crimes financeiros. As atividades incluem ações educativas e informativas, promovendo maior compreensão sobre os riscos e as boas práticas para evitar golpes pela utilização dos meios digitais.

No estado de São Paulo, ações de conscientização incluem a produção e divulgação de cartilhas contendo dicas de segurança para prevenir estelionatos virtuais. Essas cartilhas estão disponíveis no site oficial do estado e da polícia civil, e oferecem orientações sobre como proceder em caso de suspeita ou confirmação de golpes, incluindo a recomendação de registrar boletins de ocorrência.

No Paraná também é adotado medidas preventivas através de publicação de cartilhas educativas e também promove palestras através do programa institucional PCPR na Comunidade, no qual a instituição promove diversas ações de orientação à comunidade.

No Distrito Federal, a Polícia Civil também promove orientações através de cartilhas educativas à sociedade como forma de prevenir os estelionatos virtuais e via telefone. O material é disponibilizado no site da própria PC-DF.

O Piauí possui um órgão especializado nesse tipo de crime, tem se destacado em eventos e ações de combate ao crime virtual. Em 2024, sediou o 1º Workshop Estadual de Combate a Fraudes Digitais, promovendo discussões e treinamentos sobre o enfrentamento ao estelionato eletrônico. O evento reuniu especialistas da área para compartilhar estratégias e melhores práticas na proteção contra golpes digitais, reforçando a importância da conscientização coletiva.

5. CONCLUSÃO

Após a análise realizada, verificou-se que o grau de maturidade das instituições varia significativamente entre as regiões. Essas diferenças estão relacionadas não apenas ao tempo de criação das unidades especializadas, mas também à formalização administrativa, à disponibilidade de recursos tecnológicos e à capacidade de gestão dos investimentos previstos em lei orçamentária.

Os resultados indicam que o Distrito Federal e São Paulo apresentam uma estrutura organizacional mais definida para o enfrentamento ao estelionato eletrônico e os demais crimes cibernéticos, no qual incluem divisões especializadas, investimentos em ferramentas tecnológicas avançadas, como o uso de softwares de análise forense, e parcerias estratégicas com instituições como a Polícia Federal e polícias civis dos demais estados. Essas características possibilitam uma resposta mais ágil e efetiva às demandas da população.

Por outro lado, estados como Pará e Piauí, observa-se a criação recente de delegacias especializadas para esse tipo de crime ainda em processo de consolidação administrativa e técnica. No Pará, apesar da destinação de recursos no orçamento de forma expressiva, a recente criação da DECCC e o aumento nos registros de estelionato eletrônico, sugere que os investimentos ainda estão em implantação, não sendo ainda totalmente refletidos na capacidade investigativa. Já no Piauí, mesmo observando avanços estruturais, a polícia civil enfrenta limitações orçamentárias que restringem a ampliação tecnológica e até mesmo a de recursos humanos, o que pode afetar a celeridade e a capacidade de investigação de forma eficiente. No Paraná, apesar de ser a instituição mais antiga em relação aos demais estados analisados, verificamos que não houve uma evolução estrutural como as demais instituições como criações de departamentos ou delegacias especializadas.

O aumento de registros de estelionato eletrônico acompanha a extensão do uso da internet e do comércio eletrônico, mas também reflete o fortalecimento dos canais digitais de denúncia e maior conscientização da população sobre os meios de registro.

Esse diagnóstico mostra a necessidade de políticas públicas regionais que promovam a modernização tecnológica, o fortalecimento de parcerias entre instituições públicas e privadas e a formação contínua de agentes. A criação de um sistema nacional integrado de combate aos crimes cibernéticos, associado a esforços educativos para a população, é essencial para reduzir as disparidades regionais e aumentar a eficácia no enfrentamento do estelionato eletrônico em todo o Brasil.

AGRADECIMENTOS

Agradecemos à FAPESPA (Termo de outorga 046/2021), ao CNPq (Processo 307370/2022-4) e à CAPES (Processo 88881.927473/2023-01: Práxis extensionista, conhecimento pluriuniversitário e a Pós-graduação na Amazônia sul oriental. IES: (Unifesspa) pelo aporte financeiro e pelo suporte às pesquisas.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] R.S. Aguiar; L.G.A. Neto; M.R.R. Guida. Crimes Cibernéticos: análise do processo investigatório e os desafios para combatê-los. *Rev*. RevistaFT **27**: 1-27 (2023).

[2] E.S. Costa; R.C.Silva. Crimes Cibernéticos e investigação policial. *Rev. Eletrônica do Ministério Público do Piauí*. 181-196 (2021).

[3] A. A. Castro. A internet e os tipos penais que reclamam ação criminosa em público. *Rev. De Direito Eletrônico* **1:** 41-51 (2003).

[4] F.B.Marra. Desafios do Direito na Era da Internet: uma breve análise sobre os crimes cibernéticos.*Campo Jurídico*. **7**: 145-167 (2019).

[5] I.L. Andrade. *Traffic* Forense Digital Aplicada ao Combate de Crimes Cibernéticos: Uma Revisão. *Rev.Foc.* **1**: 1-27 (2024).

[6] ClearSale; Mapa da Fraude em 2023. In:_resultados 2023.(2023).Retirado em 10/10/2024 https://br.clear.sale/mapa-da-fraude .

[7] L.M.A.Junior; V.C.M. Souza; R.S. Xerez. A incidência dos cybercrimes durante a pandemia da Covid-19 no Brasil e o processo de adaptação do Código Penal a essa realidade. *Rev*. RevistaFT. **27**:1-28 (2023).

[8] Minayo, Maria Cecília de Souza. *O desafio do conhecimento: pesquisa qualitativa em saúde*. Ed Hucitec.Brasil (2014) 35-39.

[9] Lakatos, Eva Maria; Marconi, Marina de Andrade. *Fundamentos de metodologia científica*. 5. Ed. Atlas, Brasil (2003) 100-104.

[10] Gil, Antonio Carlos. *Métodos e técnicas de pesquisa social*. Ed. Atlas(2010) 28-29.

[11] Pará. Decreto nº 690/2020. *Institui a Diretoria Estadual de Combate a Crimes Cibernéticos, no âmbito da Polícia Civil do Estado do Pará, e dá outras providências*. 16 de abril de 2020. Disponível em: https://www.sistemas.pa.gov.br/sisleis/legislacao/5542/detail Retirado em 15/10/2025.

[12] Polícia Civil do Pará (PCPA). *Diretoria Estadual de Combate a Crimes Cibernéticos.* Disponível em: https://www.pc.pa.gov.br/institucional/diretoria-estadual-de-combate-a-crimes-ciberneticos. Retirado em 15/10/2024.

[13] Polícia Civil do Pará (PCPA). *Relatório de Gestão 2024*. Disponível em: https://www.pc.pa.gov.br/documento/b7b7aj. Retirado em 20/10/2025

[14] Agência Pará. *Pc promove curso de inteligência policial com técnicas para investigações judiciárias.* Disponível em: https://www.agenciapara.com.br/noticia/61027/pc-promove-curso-de-inteligencia-policial-com-tecnicas-para-investigacoes-judiciarias . Retirado em 10/11/2024

[15] Fórum Brasileiro de Segurança Pública. *Anuário Brasileiro de Segurança Pública. (2025)*.

[16] Pará. Secretaria de Estado de Planejamento e Administração. *Quadro demonstrativo das despesas por fonte de recursos – OGE 2024.*. Disponível em: https://seplad.pa.gov.br/wp-content/uploads/2024/01/QDD-2024.pdf . Retirado em: 20/10/ 2025.

[17] Secretaria de Estado de Segurança Pública e Defesa Social do Pará. *Segurança investe em tecnologia contra crimes cibernéticos*. Disponível em: https://segup.pa.gov.br/noticias/seguran%C3%A7ainveste-em-tecnologia-contra-crimes-cibern%C3%A9ticos. Retirado em 15/10/2024

[18] Agência Pará. *Divisão de Combate a Crimes Cibernéticos alerta sobre aumento de riscos de golpe online.* Disponível em: https://agenciapara.com.br/noticia/31704/divisao-de-combate-a-crimes-ciberneticos-alerta-sobre-aumento-de-riscos-de-golpes-online .Retirado em 20/10/2024

[19] Governo do Distrito Federal . *Polícia Civil apresenta delegacia que reforçará o combate aos crimes cibernéticos*. Disponível em: https://www.df.gov.br/policia-civil-apresenta-delegacia-que-reforcara-o-combate-aos-crimes-ciberneticos/. Retirado em 20/10/2024

[20] Polícia Civil do Distrito Federal (PCDF). *Organograma da Polícia Civil do Distrito Federal.* Disponível em: https://www.pcdf.df.gov.br/institucional/organograma Retirado em 20/10/2024.

[21] Polícia Civil do Distrito Federal (PCDF). *Relatório integrado de gestão – 2025*. Disponível em: https://www.pcdf.df.gov.br/images/conteudo/gci/DIPLANE/TRANSPARENCIA/REL_GEST%C3%83O_2025.pdf . Retirado em 20/10/2025.

[22] Sinpol-DF. *Polícia Civil em Foco: Como é a investigação de crimes cibernéticos por policiais civis no DF* [Vídeo].Youtube. Disponível em: https://www.youtube.com/watch?v=oZHk9AkPi7k. Retirado em 02/11/2024.

[23] Agência Brasília. *Segurança Pública do DF assina acordo com a PF para combate a crimes cibernéticos*. Governo do Distrito Federal. Disponível em: https://www.agenciabrasilia.df.gov.br/w/seguranca-publica-do-df-assina-acordo-com-a-pf-para-combate-a-crimes-ciberneticos . Retirado em 20/10/2024.

[24] Polícia Civil do Distrito Federal (PCDF). *197 Denúncia Online*. Disponível em: https://www.pcdf.df.gov.br/servicos/197. Retirado 02/11/2024.

[25] B.Rechinho; T.Chinellato; C.A.G.Silva. DCCIBER - *Divisão de Crimes Cibenéticos*. Apresentação Institucional (2023). Disponível em: https://aepremerj.com.br/wp-content/uploads/2023/07/18h00-CARLOS-AFONSO-AEPEPRERJ-APRESENTACAO-INSTITUCIONAL-DCCIBER-2023.pdf. Retirado em 04/11/2024.

[26] UOL. *Perfil da Polícia Civil do Estado de São Paulo e cenário atual*. Disponível em: https://noticias.uol.com.br/cotidiano/ultimas-noticias/2025/09/01/perfil-policia-civil-sp.htm . Retirado em 20/10/2025.

[27] Governo do Estado de São Paulo. *Policiais de SP participam de treinamento de segurança do FBI*. Governo de São Paulo. Disponível em: https://www.sp.gov.br/sp/canais-comunicacao/noticias/policiais-de-sp-participam-de-treinamento-de-seguranca-do-fbi. Retirado em 04/11/2024.

[28] Governo do Estado de São Paulo. *Crimes no ambiente virtual serão monitorados por núcleo especial*. Agência SP. Disponível em: https://www.agenciasp.sp.gov.br/crimes-no-ambiente-virtual-serao-monitorados-por-nucleo-especial/. Retirado em 18/02/2025.

[29] Governo do Estado de São Paulo. Lei nº 17.863, de 22 de dezembro de 2023. Diário Oficial do Estado de São Paulo, 26 dez. 2023. Disponível em: https://portal.fazenda.sp.gov.br/servicos/orcamento/Documents/LOA/Lei_17863_de_22_12_2023.pdf. Retirado em 20/10/2025.

[30] TecMundo. *Crimes Digitais, hackers e ciberpolícia* [Vídeo].Youtube. Disponível em: https://www.youtube.com/watch?v=keCPxQLdAEM. Retirado em 02/11/2024.

[31] Secretaria da Segurança Pública do Estado de São Paulo. *Delegacia eletrônica*. Governo do Estado de São Paulo. Disponível em: https://www.ssp.sp.gov.br/servicos/delegacia-eletronica. Retirado em 04/11/2024.

[32] GP1. *Delegacia de Repressão aos Crimes de Informática é inaugurada em Teresina.* Disponível em: https://conectapiaui.com.br/noticia/seguranca/secretario-chico-lucas-entrega-reforma-de-delegacia-contra-crimes-virtuais-em-the-3140.html. Retirado em 16/02/2025.

[33] Governo do Piauí. *Polícia Civil realiza curso de investigação policial via análise de dados telemáticos.* Disponível em: https://portal.pi.gov.br/pc/2024/04/29/policia-civil-realiza-curso-de-investigacao-policial-via-analise-de-dados-telematicos/. Retirado em 16/02/2025.

[34] Ministério Público do Estado do Piauí & Polícia Civil do Estado do Piauí. *Acordo de Cooperação Técnica nº 13/2023 – MPPI e Polícia Civil.* Disponível em: https://www.mppi.mp.br/internet/wp-content/uploads/2023/07/ACT-13.2023-MPPI-E-POL-CIVIL-SEI_19.21.0014.0003615_2020_56.pdf. Retirado em 01/12/2024.

[35] Secretaria de Estado do Planejamento do Piauí. *Lei Orçamentária Anual – LOA 2024*. Teresina (PI): SEPLAN-PI. Disponível em: https://www.seplan.pi.gov.br/loa/#94-122-wpfd-2024. Retirado em 20/10/2025.

[36] GP1. *Secretaria de Segurança do Piauí adquire software israelense para extrair dados de celulares.* Disponível em: https://www.gp1.com.br/policia/noticia/2024/2/28/secretaria-de-seguranca-do-piaui-adquire-software-israelense-para-extrair-dados-de-celulares-565736.html. Retirado em 10/12/2024.

[37] Ministério Público do Estado do Piauí. *Manual da Delegacia Eletrônica da Polícia Civil do Piauí.* Disponível em: https://www.mppi.mp.br/internet/wp-content/uploads//2020/05/manual%20delegacia%20eletronica%20pcpi.pdf. Retirado em 10/12/2024.

[38] Polícia Civil do Estado do Paraná (PCPR). *Núcleo de Combate a Crimes Cibernéticos (NUCIBER)*. Disponível em: https://www.policiacivil.pr.gov.br/NUCIBER. Retirado em 22/11/2024.

[39] Polícia Civil do Estado do Paraná (PCPR). Novos policiais civis tomam posse e reforçam o efetivo da PCPR.. Acesso em: https://www.policiacivil.pr.gov.br/Noticia/560-novos-policiais-civis-tomam-posse-e-reforcam-o-efetivo-da-PCPR. Retirado em 20/10/2025.

[40] Escola Superior da Polícia Civil do Paraná**.** *ESPC promove Curso Avançado sobre Investigação de Crimes Cibernéticos*. Escola Superior da Polícia Civil do Paraná. Disponível em: https://www.escola.pc.pr.gov.br/Noticia/ESPC-promove-

Curso-Avancado-sobre-Investigacao-de-Crimes-Ciberneticos. Retirado em 15/12/2024.
[41] Agência Estadual de Notícias. *Governo firma parceria para prevenção e combate a cibercrimes*. Governo do Paraná. Disponível em: https://www.aen.pr.gov.br/Noticia/Governo-firma-parceria-para-prevencao-e-combate-cibercrimes. Retirado em 15/12/2024.
[42] Secretaria da Fazenda do Paraná. Orçamento Anual 2024. Curitiba: SEFA. Disponível em: https://www.fazenda.pr.gov.br/Pagina/Orcamento-Anual. Retirado em 20/10/2025.
[43] Polícia Civil do Estado do Paraná. *Núcleo de Combate a Crimes Cibernéticos (NUCIBER)*. Disponível em: https://www.policiacivil.pr.gov.br/NUCIBER. Retirado em 22/11/2024.
[44] Cidade Verde. *Governo publica decreto que reestrutura a Polícia Civil e cria mais delegacias no interior do estado*. Cidade Verde. Disponível em: https://cidadeverde.com/noticias/396073/governo-publica-decreto-que-reestrutura-a-policia-civil-e-cria-mais-delegacias-no-interior-do-estado. Retirado em 17/02/2025.
[45] Governo do Estado do Paraná**.** *Portal da Transparência - Consulta de Despesas*. Transparência Paraná. Disponível em: https://www.transparencia.pr.gov.br/pte/despesas/consultalivre/listar?windowId=7b7. Retirado em 17/02/2025.
[46] Metrópoles. *SP lidera alta no país e tem 1 estelionato a cada 42 segundos em 2023.* Disponível em: https://www.metropoles.com/sao-paulo/sp-lidera-alta-no-pais-e-tem-1-estelionato-a-cada-42-segundos-em-2023. Retirado em 17/02/2024.
[47] F.Zacarias; L.Z. Freire. Crimes virtuais: análise das dificuldades e limitações ao combate. *Rev*. Jures. **16**: 29-61(2023).