REVISTA TÓPICOS
ISSN 2965-6672 | Qualis A2

CARACTERIZAÇÃO DOS CRIMES PATRIMONIAIS PRATICADOS POR MEIO CIBERNÉTICO NO ESTADO DO PARÁ, DE 2022 A 2025

CHARACTERIZATION OF PROPERTY CRIMES COMMITTED THROUGH CYBER MEANS IN THE STATE OF PARÁ, FROM 2022 TO 2025

Ciências Humanas, Ciências Sociais Aplicadas • 03/11/2026

REGISTRO DOI: 10.70773/revistatopicos/793465755

Shyrley Silva da Silva[1]

Edson Marcos Leal Soares Ramos[2]

Roberto Magno Reis Netto[3]

RESUMO

O artigo caracteriza os crimes patrimoniais praticados por meio cibernético registrados no estado do Pará no período de janeiro de 2022 a dezembro de 2025. O estudo parte da constatação de que a digitalização acelerada dos meios de pagamento reposicionou a criminalidade patrimonial brasileira, deslocando-a da subtração violenta para a obtenção fraudulenta de valores em ambiente virtual. Adota-se abordagem quantitativa, de natureza exploratória e descritiva, apoiada em pesquisa documental sobre a totalidade dos 98.039 boletins de ocorrência fornecidos pela Secretaria Adjunta de Inteligência e Análise Criminal do Pará, o que configura censo. O tratamento dos dados empregou estatística descritiva, com distribuições de frequência absoluta e relativa e cálculo de taxas de variação anual. Os resultados revelam crescimento de 72,9% no total de registros no período, com predomínio das modalidades de estelionato eletrônico, que respondem por 85,1% das ocorrências, enquanto o furto mediante fraude eletrônica alcança 14,9%. A distribuição temporal concentra 86,0% das ocorrências em dias úteis e 82,3% no intervalo das seis às dezoito horas, com pico em agosto. Conclui-se que o fenômeno acompanha a rotina econômica e demanda respostas preventivas ajustadas a esses ciclos.

Palavras-chave: Ambiente virtual; estelionato eletrônico; furto mediante fraude eletrônica; meios de pagamento; boletim de ocorrência.

ABSTRACT

This article characterizes the property crimes committed through cyber means recorded in the state of Pará between January 2022 and December 2025. The study departs from the finding that the accelerated digitalization of payment systems has repositioned Brazilian property crime, shifting it from violent appropriation

towards the fraudulent obtaining of funds in virtual environments. A quantitative, exploratory and descriptive approach was adopted, based on documentary research covering all 98,039 police reports provided by the Deputy Secretariat of Criminal Intelligence and Analysis, which constitutes a census and dispenses with sampling procedures. Data treatment relied on descriptive statistics, with absolute and relative frequency distributions and the calculation of annual variation rates. Results reveal a 72.9% increase in total records over the period, with the predominance of electronic fraud, which accounts for 85.1% of occurrences, while theft by electronic fraud reaches 14.9%. Temporal distribution concentrates 86.0% of occurrences on business days and 82.3% from 6 a.m. to 6 p.m., peaking in August. The conclusion indicates that the phenomenon follows the formal economic routine and requires preventive responses adjusted to these cycles.
Keywords: Virtual environment; online fraud; theft by electronic fraud; payment systems; police report.

1. INTRODUÇÃO

A expansão dos crimes patrimoniais praticados em ambiente digital constitui uma das transformações mais visíveis da criminalidade brasileira recente (Novais; Faria, 2026). Aquilo que antes exigia proximidade física entre autor e vítima passou a ser executado remotamente, com auxílio de dispositivos conectados e de técnicas de persuasão aplicadas a distância (Bechara; Flores, 2019; Quadros; Cruz, 2024). Maragno e Yamazato (2026) descrevem esse processo como uma verdadeira industrialização do estelionato, expressão que traduz a escala assumida pelo fenômeno e a divisão de tarefas observada entre os agentes envolvidos.

Em perspectiva internacional, a fraude eletrônica financeira figura entre as ameaças criminais de maior impacto econômico, com perdas globais estimadas em 442 bilhões de dólares em 2025, quadro associado à atuação de organizações transnacionais que operam a partir de centros de fraude estruturados (Interpol, 2026), trajetória antecipada por Kuzior *et al.* (2024) ao projetarem a expansão do mercado de crimes cibernéticos para cerca de 1 trilhão de dólares até aquele ano.

No Brasil, o problema tem grande dimensão, pois levantamento da Global Anti-Scam Alliance em parceria com a Feedzai (GASA; Feedzai, 2024) posiciona o país entre os dez que proporcionalmente mais perdem riqueza para golpes digitais em relação ao Produto Interno Bruto, e os dados obtidos pelo FBSP (2026) registram 2,2 milhões de ocorrências de estelionato em 2025.

Parte desse movimento se explica pela velocidade da digitalização financeira brasileira, advinda principalmente com o lançamento do Pix, em novembro de 2020, que ampliou de forma expressiva a base de usuários do Sistema Financeiro Nacional e consequentemente a digitalização financeira (BCB, 2023; Bustamante; Santos; Batista, 2024), alcançando ao final de 2025 o patamar de 148,13 milhões de usuários pessoas físicas e 35,3 trilhões de reais movimentados, escala que o próprio Banco Central associa ao uso crescente do arranjo como canal de distribuição de fraudes e golpes (BCB, 2026).

A resposta legislativa veio com a Lei Nº 14.155, de 27 de maio de 2021 (Brasil, 2021), que inseriu qualificadoras específicas para o furto mediante fraude eletrônica, no Art. 155, § 4º-B, e para o estelionato praticado por meio eletrônico, no Art. 171, § 2º-A, ambos do Código Penal (Brasil, 1940), alterações apontadas por Evangelista e Silva

(2025) como marco relevante, ainda que apenas 2,8% das ocorrências de estelionato registradas em 2025 tenham originado processos criminais (FBSP, 2026).

O estado do Pará reúne condições que tornam particularmente relevante essa análise, pois, sendo a segunda maior unidade federativa do país em termos territoriais (IBGE, 2023), impõe desafios à distribuição territorial de estruturas policiais especializadas, os quais se somam ao resultado de estudo comparativo das condições de investigação do estelionato eletrônico em cinco unidades federativas, uma por região do país, que identificou diferentes graus de maturidade entre as instituições analisadas e concluiu pela necessidade de criação de um sistema integrado de combate aos crimes cibernéticos, acompanhado de políticas voltadas à modernização tecnológica e à formação continuada dos agentes (Oliveira; Gomes, 2026).

Desta forma, o objetivo deste artigo é caracterizar os crimes patrimoniais praticados por meio cibernético no estado do Pará no período de 2022 a 2025, quanto à evolução anual por tipo penal e à distribuição temporal das ocorrências.

2. FUNDAMENTAÇÃO TEÓRICA

A criminalidade patrimonial brasileira consolidou, ao longo de décadas, repertórios apoiados na presença física e na coação direta, a exemplo dos assaltos a agências bancárias praticados por quadrilhas com homens armados, utilizando armamento de grosso calibre e explosivos, com domínio temporário de bairros ou de cidades inteiras, modalidade que envolve planejamento minucioso, investimento em infraestrutura e recrutamento de novos

integrantes para cada operação, além do deslocamento territorial e da exposição ao risco de confronto com as forças de segurança pública (Aquino, 2023; Ferreira; Teixeira Júnior, 2025).

A digitalização das relações econômicas alterou a base material sobre a qual essa criminalidade se assentava, pois a expansão do acesso à internet produziu efeitos positivos e significativos sobre a dinâmica comercial, evidência de que a conectividade passou a mediar parcela crescente dos fluxos econômicos (Carmo, 2022; Leal, 2023), processo aprofundado pela pandemia de covid-19, que alterou padrões de consumo e acelerou a adesão a canais digitais em diferentes contextos, deslocando o dinheiro do físico para o digital (Hu *et al*., 2022; Park *et al*., 2022).

No sistema de pagamentos, essa transformação assumiu contornos próprios. A análise dos dados públicos do Banco Central do Brasil indica redução no uso dos demais instrumentos de pagamento após o lançamento do Pix, crescimento que não se explica apenas pela substituição dos meios tradicionais, mas também pela ampliação do número de pessoas com relacionamento bancário e pela substituição do dinheiro em espécie, mudanças atribuídas a um ambiente progressivamente mais inclusivo e competitivo (Sampaio; Ferreira; Securato, 2025; BCB, 2026), movimento acompanhado por investimentos contínuos do setor bancário em soluções de autenticação, monitoramento de canais digitais e detecção de padrões anômalos (Febraban, 2025).

A criminalidade acompanhou esse deslocamento de modo consistente com o que a literatura criminológica já havia observado, uma vez que cada estágio de desenvolvimento tecnológico molda as formas de criminalidade que nele emergem, deslocando

progressivamente o crime informático clássico para o cibercrime de alcance ampliado (Choi; Lee; Louderback, 2020), transição cuja singularidade reside no anonimato e na dissociação entre identidade física e identificação virtual, condições que alimentam a percepção de relativa impunidade e configuram o estado anômico característico dessas modalidades delitivas (Suxberger; Pacheco, 2019).

Esse deslocamento materializou-se, sobretudo, em duas modalidades de crimes patrimoniais, às quais a Lei N° 14.155/2021 (Brasil, 2021) conferiu tratamento específico ao introduzir as qualificadoras do furto mediante fraude eletrônica, no Art. 155, § 4°-B, e do estelionato eletrônico, no Art. 171, § 2°-A, do Código Penal (Brasil, 1940; Evangelista; Silva, 2025). Embora ambas empreguem recursos digitais, sua distinção jurídica depende da forma como ocorre a movimentação patrimonial e do papel desempenhado pela vítima na execução do delito (Masson, 2026; Prado, 2025).

No furto mediante fraude eletrônica, a subtração ocorre à revelia da vítima, mediante dispositivo eletrônico ou informático, conectado ou não à rede, com ou sem violação de mecanismos de segurança ou emprego de programa malicioso (Lai; Mourão, 2021; Cunha, 2023). Entre os meios utilizados está o *malware*, programa instalado de forma dissimulada que permite ao agente acessar remotamente dados ou executar transferências sem o conhecimento do titular (Gopinath; Sethuraman, 2023; Ribeiro; Cordeiro; Fumach, 2022).

No estelionato eletrônico, por sua vez, o engano interfere na formação da vontade da vítima, levando-a a fornecer informações ou a realizar voluntariamente o ato de disposição patrimonial por meio de redes sociais, contatos telefônicos, sítios falsos ou recursos digitais

análogos (Santos; Sotero, 2024; Prado, 2025). A capacidade de persuasão dessas abordagens pode ser ampliada pelo emprego de *deepfakes*, conteúdos audiovisuais sintéticos capazes de simular, com verossimilhança, vozes e imagens reais (Oliveira; Ávila, 2024; Sousa *et al*., 2025).

A diferenciação entre essas modalidades evidencia duas dimensões da criminalidade patrimonial digital: no furto, predomina a exploração de vulnerabilidades técnicas ou a neutralização da vigilância, enquanto, no estelionato, prevalece a manipulação da percepção e da vontade da vítima (Capez, 2025; Greco, 2024; Prado, 2025). Nesse contexto, a engenharia social compreende estratégias de persuasão e exploração da confiança destinadas a induzir comportamentos favoráveis ao agente, constituindo elemento explicativo da maior ocorrência de delitos que dependem da colaboração da própria vítima (Quadros; Cruz, 2024; Santos; Miranda; Reis Netto, 2023).

A proximidade entre os tipos penais também pode dificultar o enquadramento inicial quando o relato não permite determinar se a vítima realizou voluntariamente a transferência ou se o valor foi subtraído sem seu conhecimento (Cunha, 2023; Capez, 2025). Por isso, a distinção conceitual apresentada fornece o suporte necessário para interpretar a evolução dos registros efetuados pela Polícia Civil no Estado do Pará no período de janeiro de 2022 a dezembro de 2025.

3. METODOLOGIA

A investigação adota abordagem quantitativa. Conforme Creswell e Creswell (2021), essa vertente busca explicar fenômenos por meio da

mensuração e da comparação entre variáveis. Quanto aos objetivos, a pesquisa é descritiva, pois se propõe a detalhar o fenômeno investigado (Creswell; Creswell, 2021), e exploratória, por se dirigir a objeto pouco investigado no plano estadual (Gil, 2022). Quanto aos procedimentos técnicos, combina pesquisa bibliográfica, apoiada em livros, artigos, dissertações e relatórios institucionais, e pesquisa documental, sobre a base de boletins de ocorrência policial, classificável como documento de segunda mão (Gil, 2022).

O lócus da pesquisa é o estado do Pará, situado na região Norte do Brasil, com área territorial de 1.245.870,707 quilômetros quadrados, o que corresponde a aproximadamente 14,6% do território nacional e o coloca como segunda maior unidade federativa do país com 144 municípios e população estimada em 8.116.132 habitantes (IBGE, 2023), apresentando diversidade sociocultural e econômica que influencia tanto a dinâmica criminal quanto a capacidade operacional dos órgãos de segurança pública.

A delimitação temporal da pesquisa considera que as qualificadoras específicas foram introduzidas no Código Penal (Brasil, 1940) pela Lei Nº 14.155, de 27 de maio de 2021 (Brasil, 2021), de modo que o período de 2022 a 2025 permite acompanhar a evolução dos registros já sob a vigência plena das novas qualificadoras, afastando a distorção dos meses iniciais de adaptação dos procedimentos de classificação policial.

Os dados analisados neste estudo foram fornecidos pela Secretaria Adjunta de Inteligência e Análise Criminal (SIAC), vinculada à Secretaria de Estado de Segurança Pública e Defesa Social do Pará (SEGUP-PA). Foi disponibilizada planilha eletrônica com 98.039 registros de boletins de ocorrência relativos a três situações típicas,

no caso, o estelionato enquadrado no caput do Art. 171 do Código Penal, porém praticado por meio eletrônico; estelionato eletrônico previsto no Art. 171, § 2º-A; e furto mediante fraude eletrônica previsto no Art. 155, § 4º-B, todos do Código Penal (Brasil, 1940).

Utilizou-se a totalidade dos registros disponíveis, o que caracteriza censo e afasta a necessidade de procedimentos amostrais, bem como a estimação de erros de amostragem. Cumpre esclarecer que a categoria denominada estelionato na base oficial reúne ocorrências enquadradas no caput do Art. 171 do Código Penal (Brasil, 1940) cuja execução se deu por meio eletrônico, enquanto a categoria fraude eletrônica corresponde estritamente à qualificadora do § 2º-A. A distinção é registral e não altera a natureza jurídica das condutas, mas permite observar o processo de incorporação da figura qualificada à rotina de classificação policial.

A coleta seguiu quatro etapas sucessivas. A primeira consistiu na obtenção e na organização da base estatística encaminhada pela Secretaria Adjunta de Inteligência e Análise Criminal, referente ao intervalo de janeiro de 2022 a dezembro de 2025. Na segunda, os registros foram submetidos a tratamento preliminar no software Microsoft Excel, com padronização de rótulos, limpeza de campos inconsistentes, verificação de duplicidades e conferência dos totais por ano e por tipo penal, tendo-se optado por preservar tanto as ocorrências consumadas quanto as tentadas, pois ambas expressam a exposição efetiva da população ao risco.

Na terceira etapa, foram selecionadas as variáveis pertinentes ao objetivo de caracterização: ano do fato, de 2022 a 2025; mês do fato, de janeiro a dezembro; dia da semana do fato, de domingo a sábado; faixa de horário do fato, em quatro intervalos de seis horas;

fato típico, distinguindo estelionato praticado por meio eletrônico, estelionato eletrônico e furto mediante fraude eletrônica; e unidade policial responsável pelo registro.

Na quarta, as variáveis foram tabuladas em planilhas de distribuição de frequência, com apuração de frequências absolutas e relativas e cálculo das taxas de variação anual segundo a razão entre a quantidade observada no ano corrente e a do ano anterior, resultado que serviu de base para os gráficos de colunas apresentados na seção seguinte.

A pesquisa utilizou dados secundários, fornecidos pela SIAC, os quais vieram anonimizados e agregados, sem possibilidade de identificação individual. Ainda assim, todas as etapas de tratamento observaram cuidados quanto à anonimização integral das informações, em conformidade com a Lei Geral de Proteção de Dados, Lei nº 13.709, de 14 de agosto de 2018 (Brasil, 2018).

O acesso às informações respeitou os parâmetros da Lei Nº 12.527, de 18 de novembro de 2011 (Brasil, 2011), que assegura o direito de acesso a dados públicos ao mesmo tempo que resguarda as hipóteses de sigilo e as restrições relativas a dados pessoais, de modo que a obtenção e o uso das informações junto aos órgãos de segurança pública observaram tais limites legais (Bioni; Silva; Martins, 2022).

4. RESULTADOS E DISCUSSÕES

4.1. Evolução Anual e Composição por Tipo Penal

A Tabela 1 apresenta a quantidade de ocorrências de crimes patrimoniais cibernéticos registradas pela Polícia Civil do estado do

Pará no período de 2022 a 2025, acompanhada das taxas de variação percentual anual por tipo penal.

Tabela 1. Quantidade de ocorrências de crimes patrimoniais cibernéticos e variação percentual anual, registrados pela polícia civil do estado do Pará, de 2022 a 2025.

Tipo de Crime	Ano				Tota
	2022	2023	2024	2025	
Estelionato	13.861	18.144	19.472	20.718	72
Fraude Eletrônica	2	1.628	4.199	5.362	1
Furto	3.782	2.797	3.645	4.429	14

⚠ Esta tabela possui muitas colunas e foi cortada para impressão. Para visualizá-la completa, acesse o artigo original em: https://revistatopicos.com.br/artigos/caracterizacao-dos-crimes-patrimoniais-praticados-por-meio-cibernetico-no-estado-do-para-de-2022-a-2025?noblockage

Fonte: Elaborado pelos autores a partir de dados da SIAC, outubro/2026.

Observa-se na Tabela 1 que o total de registros passou de 17.645 ocorrências em 2022 para 30.509 em 2025, representando crescimento de 72,9% no período analisado. Entretanto, a intensidade desse crescimento não foi constante. A variação foi de 27,91% no período de 2022 a 2023, de 21,03% no período de 2023 a 2024 e de 11,69% no período de 2024 a 2025, indicando desaceleração progressiva do ritmo de crescimento dos registros.

A desaceleração observada comporta ao menos três hipóteses, que os dados disponíveis não permitem testar. A primeira decorre da própria natureza da fonte, pois se trata de crimes reportados e não necessariamente de crimes cometidos, de modo que a subnotificação, recorrente nos delitos patrimoniais, dificulta distinguir entre redução efetiva do fenômeno e redução apenas do volume registrado (Almeida *et al.*, 2023).

A segunda hipótese relaciona-se à condição particular da vítima dessas modalidades, uma vez que a vergonha e a autoculpabilização decorrentes de ter sido enganada inibem o reporte do fato às autoridades, contribuindo para a formação da cifra oculta desses delitos (Campelo; Jayme, 2023). A terceira remete à ausência de padronização dos procedimentos de registro criminal entre as unidades da Federação, cabendo a cada polícia civil definir a forma de coleta e sistematização das ocorrências (IPEA, 2025).

Somadas, as categorias estelionato e fraude eletrônica, correspondentes, respectivamente, à forma básica e à modalidade qualificada do crime previsto no art. 171 do Código Penal, totalizam 83.386 ocorrências, equivalentes a 85,05% dos registros analisados. Por sua vez, o furto mediante fraude eletrônica representa 14.653 registros, correspondentes a 14,95% do total.

Essa distribuição evidencia a predominância dos registros classificados como estelionato e fraude eletrônica, que concentram 85,05% das ocorrências. O resultado sugere maior participação, no conjunto analisado, de práticas fraudulentas caracterizadas pela indução ou manutenção da vítima em erro, em comparação com aquelas em que a fraude é empregada para viabilizar a subtração patrimonial sem que a vítima tenha consciência do ato de

subtração. Essa interpretação, contudo, deve considerar os critérios de classificação das ocorrências e não permite, isoladamente, concluir sobre a dinâmica efetiva de todos os crimes registrados.

Considerando a distinção doutrinária entre estelionato eletrônico e furto mediante fraude eletrônica (Masson, 2026; Prado, 2025), os resultados indicam que as ocorrências registradas no estado do Pará concentram-se, majoritariamente, na modalidade na qual a obtenção da vantagem patrimonial depende da manipulação da percepção ou da vontade da vítima, fazendo uso de técnicas de engenharia social. Esse padrão mostra-se compatível com o cenário nacional, no qual o estelionato figura entre os principais delitos patrimoniais registrados pelas instituições de segurança pública (FBSP, 2026).

A categoria fraude eletrônica, correspondente à forma qualificada prevista no art. 171, § 2º-A, do Código Penal (Brasil, 1940) e introduzida pela Lei nº 14.155/2021 (Brasil, 2021), passou de apenas 2 ocorrências em 2022 para 1.628 em 2023, 4.199 em 2024 e 5.362 em 2025. Ao se considerar a participação de cada categoria no total de registros do respectivo ano, observa-se que o estelionato, embora tenha crescido em números absolutos, passou de 78,6% das ocorrências em 2022 (13.861 de 17.645) para 67,9% em 2025 (20.718 de 30.509), ao passo que a fraude eletrônica, que representava apenas 0,01% em 2022 (2 registros), alcançou 17,6% em 2025 (5.362 registros).

Observa-se, portanto, que o registro da forma qualificada vem sendo gradualmente incorporado à rotina de classificação policial, refletindo migração classificatória interna ao mesmo tipo penal.

Assim, uma hipótese é que essa variação entre essas categorias pode refletir a forma como a Polícia Civil no estado do Pará define seus procedimentos de coleta e sistematização das ocorrências, uma vez que não há padronização dos registros criminais entre as unidades da Federação (IPEA, 2025).

Diante disso, caso as condutas registradas na categoria estelionato tenham sido praticadas nas condições descritas no art. 171, § 2º-A, do Código Penal, como sinalizado nos dados fornecidos pela SIAC, seria esperado que, após a entrada em vigor da Lei nº 14.155/2021 (Brasil, 2021), fossem classificadas na correspondente figura qualificada, e não no caput do dispositivo, já que, segundo Marinho e Freitas (2014), as qualificadoras constituem elementares adicionais que se agregam ao tipo básico para formar um tipo derivado e influem diretamente na tipificação do fato. A eventual ausência desse ajuste na rotina de classificação policial pode comprometer a qualidade dos dados estatísticos produzidos a partir dos boletins de ocorrência, reduzindo a precisão com que representam a incidência das modalidades investigadas (Marcineiro *et al.*, 2022).

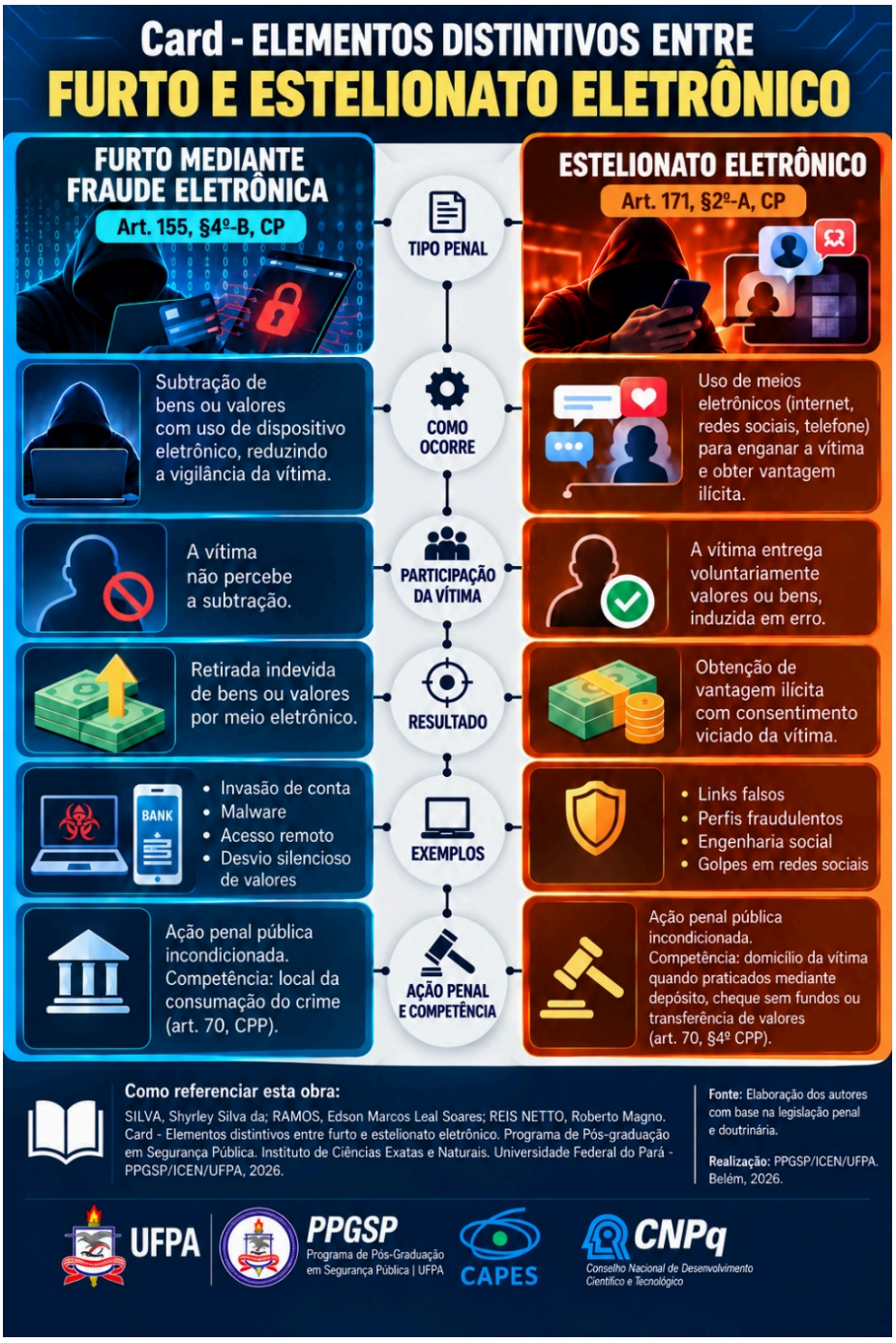
O furto mediante fraude eletrônica, conforme demonstra a Tabela 1, apresentou redução de 26,04% no período de 2022 a 2023, passando de 3.782 para 2.797 ocorrências. Nos anos seguintes, contudo, observou-se crescimento de 30,32% em 2024 e de 21,51% em 2025, alcançando 4.429 registros ao final da série, o que representa aumento acumulado de 17,1% em relação ao primeiro ano analisado. Uma possível explicação para esse comportamento está na dificuldade de distinguir o furto mediante fraude eletrônica do estelionato eletrônico no momento do registro, especialmente quando o relato da vítima não permite identificar com clareza se

houve entrega voluntária do valor ou subtração sem seu conhecimento.

Tendo em vista essa complexidade que pode envolver a classificação adequada dos casos de furto mediante fraude eletrônica e de estelionato eletrônico, especialmente quanto à identificação da participação da vítima no processo fraudulento, recomenda-se a promoção de capacitação periódica dos escrivães da Polícia Civil acerca dos elementos que distinguem essas modalidades criminosas, contribuindo para o aprimoramento da precisão e da confiabilidade dos registros policiais.

Como produto técnico decorrente desta pesquisa, foi elaborado um card informativo destinado a esclarecer elementos distintivos dessas duas modalidades criminosas (Silva; Ramos; Reis Netto, 2026). O material destina-se a profissionais da segurança pública, à comunidade acadêmica e à população em geral, apresentando, de forma didática, as principais características de cada delito. Busca-se, assim, contribuir para o correto enquadramento jurídico dos fatos no momento do registro do Boletim de Ocorrência, além de auxiliar na elucidação de dúvidas recorrentes sobre a distinção entre essas duas espécies de crimes patrimoniais praticados por meio cibernético.

Figura 1. Card - Elementos distintivos entre furto e estelionato eletrônico.



Fonte: Silva; Ramos; Reis Netto, 2026.

4.2. Registros Concentrados na Diretoria Estadual de Combate a Crimes Cibernéticos da Polícia Civil do Estado do Pará

A Tabela 2 mostra os registros lavrados na Diretoria Estadual de Combate a Crimes Cibernéticos (DECCC), da Polícia Civil do estado do Pará, permitindo comparação com o conjunto estadual apresentado anteriormente.

Tabela 2. Quantidade de ocorrências de crimes patrimoniais cibernéticos e variação percentual anual, registrados pela DECCC da Polícia Civil do estado do Pará, de 2022 a 2025.

Tipo de Crime	Ano				Tota
	2022	2023	2024	2025	
Estelionato	1.817	2.621	2.120	2.237	72
Fraude Eletrônica	0	28	248	73	1
Furto	151	26	148	128	14

⚠ Esta tabela possui muitas colunas e foi cortada para impressão. Para visualizá-la completa, acesse o artigo original em: https://revistatopicos.com.br/artigos/caracterizacao-dos-crimes-patrimoniais-praticados-por-meio-cibernetico-no-estado-do-para-de-2022-a-2025?noblockage

Fonte: Elaborado pelos autores a partir de dados da SIAC, outubro/2026.

A DECCC concentrou 9.597 registros no período analisado, o equivalente a 9,79% do total estadual de 98.039 ocorrências. A comparação entre as Tabelas 1 e 2 revela comportamento distinto entre a série estadual e a série observada nesta diretoria especializada. Enquanto o volume total de registros no estado do Pará apresentou crescimento contínuo no período de 2022 a 2025, os registros da DECCC atingiram o ponto mais elevado em 2023, com 2.675 ocorrências, e passaram a apresentar retração nos dois anos subsequentes, com reduções de 5,94% em 2024 e de 3,10% em 2025, quando foram contabilizados 2.438 registros. Como

consequência, a participação da diretoria no total estadual reduziu-se de 11,85% em 2023 para 8,00% em 2025.

Os dados disponíveis não permitem identificar as causas dessa retração dos registros na DECCC, mas admitem a formulação de hipóteses. Uma delas é que a unidade tenha alcançado o limite de sua capacidade operacional diante da crescente demanda, situação já observada em delegacias especializadas em crimes cibernéticos no país, que lidam com elevado volume de ocorrências e enfrentam dificuldades relacionadas à padronização dos procedimentos de atendimento inicial (Brochado, 2025).

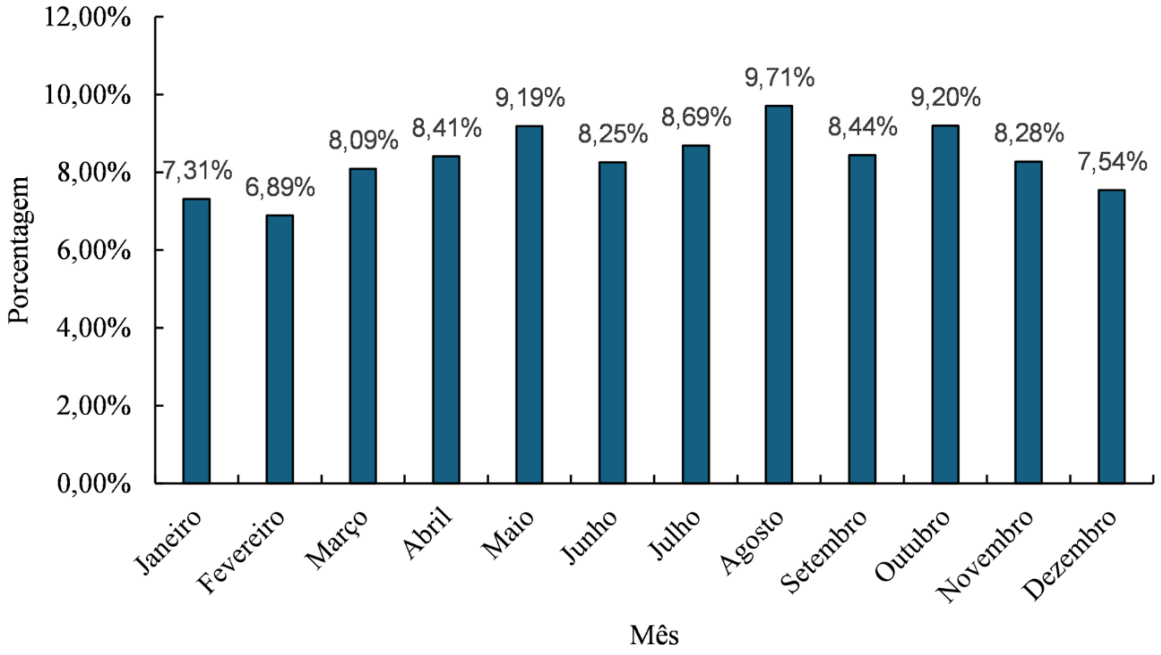
Outra hipótese é que os critérios internos de recebimento tenham priorizado casos de maior gravidade ou de reiteração, em detrimento de ocorrências pontuais. Esse tipo de mecanismo já foi documentado internacionalmente em unidades de perícia digital na Inglaterra, que adotam matrizes formais de priorização para decidir quais casos recebem exame aprofundado diante do descompasso entre a demanda e a capacidade de atendimento (Wilson-Kovacs; Wilcox, 2023), padrão que também se manifesta entre unidades especializadas de investigação cibernética, cujas capacidades variam consideravelmente e nas quais policiais frequentemente priorizam crimes de rua em detrimento de casos cibernéticos (Steinmetz *et al.*, 2024), o que reduziria o volume registrado sem indicar menor demanda real.

As categorias de Fraude eletrônica e furto mediante fraude eletrônica, em contraste, têm participação bem menor, somando 349 e 453 registros no total dos quatro anos, sem uma tendência clara de aumento ou de redução ao longo do tempo, o que impossibilita determinadas análises.

4.3. Distribuição Temporal das Ocorrências

Esta seção do estudo analisa a distribuição por mês, por dia da semana e por faixa de horário, tratadas em conjunto porque, como se verá a seguir, os gráficos apontam na direção de que o crime patrimonial cibernético acompanha a rotina econômica formal.

Figura 2. Percentual de registros somados de estelionato eletrônico e furto mediante fraude eletrônica, ocorridos no estado do Pará, por Mês, no período de 2022 a 2025.



Fonte: Construção dos autores a partir de dados do SIAC, outubro/2026.

Conforme observa-se, a distribuição mensal apresenta amplitude moderada, variando de 6,89% em fevereiro a 9,71% em agosto, diferença de 2.770 ocorrências entre o mês de menor e o de maior incidência. Esta relativa uniformidade pode indicar que, no Pará, esses crimes patrimoniais praticados por meio cibernético não dependem de eventos pontuais, mas acompanham o funcionamento ordinário da economia. Ainda assim, merecem destaque os meses de agosto, com 9.520 registros e 9,71% do total;

outubro, com 9.020 registros, correspondente a 9,20%; e maio, com 9.007 e 9,19%.

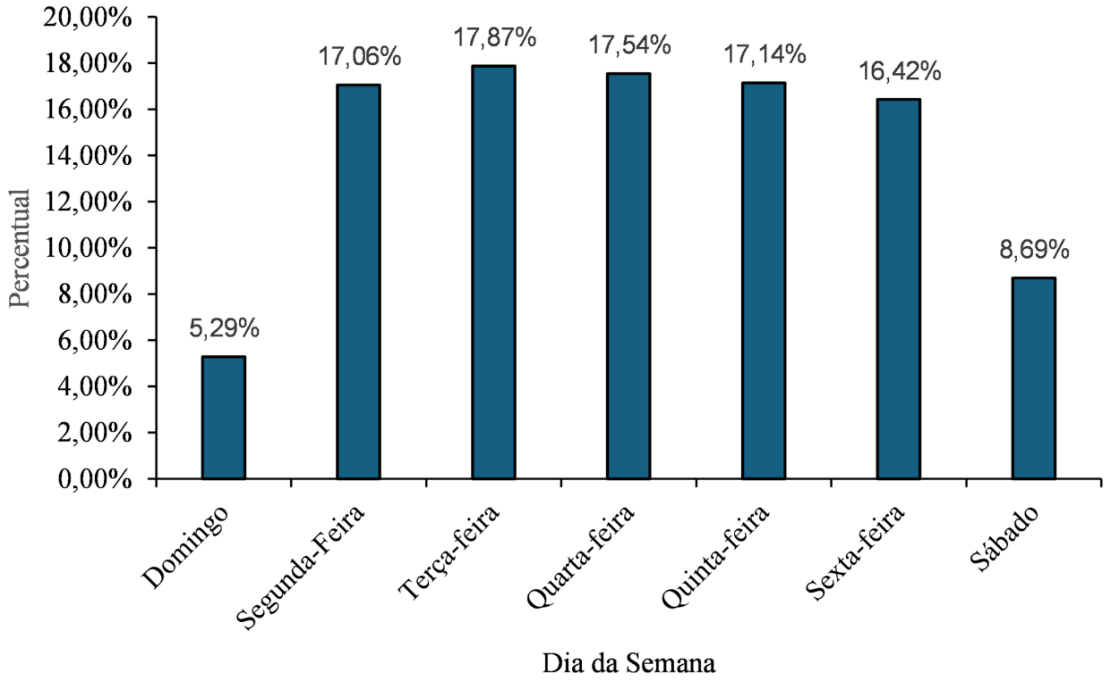
Os meses de maio e outubro admitem hipóteses específicas para o contexto paraense. Maio concentra o Dia das Mães, data em que levantamento da Serasa Experian identificou o maior risco proporcional de fraude entre as principais datas comemorativas do varejo brasileiro, com taxa 8,3% acima da média anual do setor (Serasa Experian, 2025).

Outubro, por sua vez, coincide com o Círio de Nazaré, maior manifestação religiosa do estado, cujo impacto econômico sobre a Região Metropolitana de Belém foi documentado em pesquisa acadêmica que estimou, em 2024, impacto direto de R$ 189 milhões gerado pelo evento (Magalhães, 2025), cenário que amplia o volume de transações financeiras e o fluxo de visitantes na capital paraense, condições que podem favorecer a atuação de agentes fraudadores e ajudam a explicar a concentração de registros de crimes patrimoniais cibernéticos observada nesse mês.

Em contraste, os dados oficiais do IBGE sobre o volume de vendas no comércio varejista ampliado no Brasil, no período de janeiro de 2022 a dezembro de 2025, mostram dezembro como o mês de maior movimentação em todos os quatro anos da série, seguido por novembro, o que indica que o pico da criminalidade patrimonial cibernética no Pará não acompanha diretamente o pico do comércio varejista ampliado nacional (IBGE, 2026).

A Figura 2 apresenta a distribuição das ocorrências segundo o dia da semana em que os crimes analisados ocorreram.

Figura 3. Percentual de registros somados de estelionato eletrônico e furto mediante fraude eletrônica, ocorridos no estado do Pará, por dia da semana, no período de 2022 a 2025.



Fonte: Construção dos autores a partir de dados do SIAC, outubro/2026.

Os cinco dias úteis concentram 84.333 ocorrências, ou 86,02% do total, enquanto sábado e domingo reúnem 13.706 registros, ou 13,98%. Considerando o total acumulado no período, cada dia útil reuniu, em média, 16.867 registros, enquanto cada dia do fim de semana apresentou média de 6.853 ocorrências.

O domingo isolado responde por apenas 5,29% do total, ou seja, menos de um terço do volume observado na terça-feira, dia de maior incidência com 17,87%.

Entre os dias úteis, a variação é pequena e decrescente ao longo da semana, de 17,87% na terça para 16,42% na sexta. O resultado é coerente com o achado de Silva (2020) quanto à concentração de cibercrimes em dias de maior movimentação bancária e comercial no estado do Pará, ainda que o presente estudo identifique como

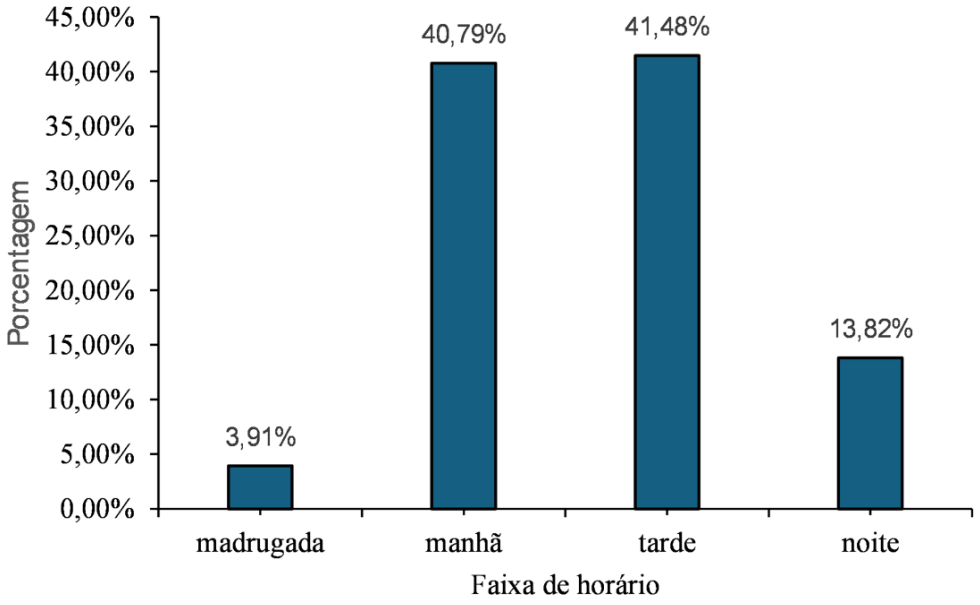
pico a terça-feira, e não a segunda, o que pode decorrer do escopo mais amplo aqui adotado.

Uma hipótese que explica este padrão é que o agente criminoso escolhe deliberadamente os dias úteis porque é neles que circula o maior volume de recursos e que a vítima considera verossímil o contato de uma instituição financeira ou de um estabelecimento comercial. A outra hipótese é que a data informada no boletim corresponde ao momento em que a vítima percebe que foi vítima de golpe ou fraude eletrônica.

Para fins de planejamento operacional, essa constatação também é útil, pois a literatura internacional sobre dimensionamento de efetivo policial defende que o número de policiais alocados deve ser definido a partir da demanda real de atendimentos, e não por critérios genéricos como um número fixo de policiais por habitante, de modo que conhecer os dias de maior volume de registros ajuda a distribuir melhor as equipes entre os turnos de trabalho (Wilson; Grammich, 2024).

A Figura 4 apresenta gráfico de colunas com a distribuição das ocorrências por turno, completando a caracterização temporal do fenômeno.

Figura 4. Percentual de registros somados de estelionato eletrônico e furto mediante fraude eletrônica, ocorridos no estado do Pará, por turno, no período de 2022 a 2025.



Fonte: Construção dos autores a partir de dados do SIAC, outubro/2026.

Observa-se a concentração diurna dos registros, uma vez que que os turnos da manhã e tarde reúnem 80.654 ocorrências, ou 82,27% do total, com equilíbrio entre manhã (40,79%) e tarde (41,48%), enquanto o período noturno responde por 13,82% e a madrugada por apenas 3,91%, equivalente a 3.838 registros ao longo dos quatro anos, reforçando a conclusão extraída da análise semanal acima.

A constatação contraria a ideia de que o ambiente digital, sempre disponível, tornaria irrelevante o horário em que o crime ocorre, pois, evidências recentes mostram que os criminosos cibernéticos concentram suas ações justamente durante o horário comercial para que a atividade fraudulenta se confunda com o volume normal de transações e passe despercebida (Madarie; Weulen Kranenbarg; De Poot, 2025). Portanto, o crime patrimonial cibernético não se descolou da rotina econômica formal, apenas migrou o meio de execução, mantendo um padrão de distribuição temporal que independe do local físico da vítima (Novais; Faria, 2026).

5. CONCLUSÃO

Os registros dos crimes patrimoniais praticados por meio cibernético no estado do Pará crescem de forma sustentada, porém em ritmo decrescente, com expansão de 72,9% no período de 2022 a 2025 e taxas anuais que recuam de 27,91% para 11,69% ao longo da série. O objetivo geral proposto na introdução foi atingido, na medida em que o estudo caracterizou o fenômeno quanto à evolução anual, à composição por tipo penal e à distribuição temporal das ocorrências.

A modalidade de estelionato eletrônico predomina no estado, concentrando 85,1% dos registros analisados. Considerando a distinção jurídica entre estelionato eletrônico e furto mediante fraude eletrônica, os resultados sugerem maior incidência de ocorrências em que a obtenção da vantagem patrimonial decorre da indução da vítima a erro, usando técnicas de engenharia social, do que de situações em que a subtração ocorre sem seu conhecimento.

Esse resultado pode contribuir para orientar políticas de prevenção e campanhas de conscientização promovidas pelos órgãos de segurança pública e pelas instituições financeiras, especialmente aquelas voltadas à identificação de tentativas de golpe, à educação do usuário e à adoção de mecanismos adicionais de confirmação em operações de transferência.

O fenômeno acompanha a rotina econômica formal, de modo que os dias úteis concentram 86,0% das ocorrências e o intervalo das seis da manhã às dezoito horas reúne 82,3%, o que recomenda o dimensionamento dos plantões de atendimento e dos fluxos de bloqueio segundo esse ciclo. A variação mensal é moderada e apresenta pico em agosto, seguido de outubro e maio, não

apresentando picos nos meses de novembro e dezembro, considerados os meses de maior volume de vendas no comércio varejista ampliado no Brasil.

A DECCC concentrou 9,79% dos registros do período, com trajetória descendente desde 2023, em direção oposta à do total estadual. As causas dessa retração não podem ser determinadas com os dados disponíveis, mas são compatíveis com hipóteses já documentadas na literatura sobre o volume de demanda superior à capacidade de atendimento de unidades especializadas de crimes cibernéticos, e a priorização de casos conforme critérios internos de gravidade ou reiteração.

Some-se a essa caracterização o achado de que parcela expressiva dos registros de estelionato praticado por meio eletrônico permanece classificada fora da forma qualificada do § 2º-A do Art. 171 do Código Penal (Brasil, 1940), apesar de o meio eletrônico empregado constituir elemento relevante para a classificação na forma qualificada, considerando também que a definição jurídica adequada depende da dinâmica concreta da conduta e do papel desempenhado pela vítima.

Considerando também a possível dificuldade prática de distinguir o furto mediante fraude eletrônica do estelionato eletrônico, tarefa que exige a compreensão do papel exercido pela vítima na dinâmica da fraude, recomenda-se que os escrivães da Polícia Civil recebam instrução continuada sobre as características que diferenciam essas figuras típicas derivadas, de modo a assegurar maior fidedignidade aos dados produzidos.

No mais, esse estudo oferece a caracterização estatística do conjunto de registros de crimes patrimoniais cibernéticos em todo o território paraense no período analisado, suprindo lacuna identificada na produção científica do campo da segurança pública e fornecendo subsídios ao planejamento operacional da Polícia Civil e à formulação de políticas de prevenção.

REFERÊNCIAS BIBLIOGRÁFICAS

ALMEIDA, F.; LOGSDON, L.; CECCATO, V.; DE PAULA, D.; SANTOS, J.; PORTELA, A. Análise temporal de roubos e furtos a residência em Cuiabá, Brasil. **Revista Brasileira de Segurança Pública,** São Paulo, v. 17, n. 1, p. 208-231, 2023. DOI: 10.31060/rbsp.2023.v17.n1.1456. Disponível em: https://doi.org/10.31060/rbsp.2023.v17.n1.1456. Acesso em: 24 set. 2026.

AQUINO, J. P. D. de. Abordagens truculentas e domínio de cidades brasileiras em assaltos contra bancos mediante planejamento minucioso. **Sociologias,** Porto Alegre, v. 25, n. 62, e-soc118176, p. 1-34, 2023. DOI: 10.1590/18070337-118176. Disponível em: https://www.scielo.br/j/soc/a/sNWh46wtcgtsgb4DpfKfrgd/abstract/?lang=pt. Acesso em: 24 set. 2026.

BCB. Banco Central do Brasil. **Relatório de Economia Bancária 2023.** Brasília: BCB, 2023. Disponível em: https://www.bcb.gov.br/content/publicacoes/relatorioeconomiabancaria/reb2023p.pdf. Acesso em: 24 set. 2026.

BCB. Banco Central do Brasil. **Relatório de Gestão do Pix 2023-2025.** Brasília: BCB, 2026. Disponível em: https://www.bcb.gov.br/content/estabilidadefinanceira/pix/relatorio_de_gestao_pix/relatorio_gestao_pix_2026.pdf. Acesso em: 24 set. 2026.

BECHARA, F. R.; FLORES, D. M. Crimes cibernéticos: qual é o lugar do crime para fins de aplicação da pena e determinação da competência jurisdicional? **Revista Direito Mackenzie,** São Paulo, v. 13, n. 2, p. 1-21, 2019. DOI: 10.5935/2317-2622/direitomackenzie.v13n213357. Disponível em: https://editorarevistas.mackenzie.br/index.php/rmd/article/view/13357. Acesso em: 24 set. 2026.

BIONI, B. R.; SILVA, P. G. F.; MARTINS, P. B. L. Intersecções e relações entre a Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação (LAI): análise contextual pela lente do direito de acesso. **Cadernos Técnicos da CGU,** Brasília, v. 1, p. 8-19, 15 mar. 2022. Disponível em: https://revista.cgu.gov.br/Cadernos_CGU/article/view/504. Acesso em: 24 set. 2026.

BRASIL. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940.** Código Penal. Diário Oficial da União, Rio de Janeiro, 31 dez. 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 24 set. 2026.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011.** Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal. Diário Oficial da União, Brasília, DF, 18 nov. 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 24 set. 2026.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em:

https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 24 set. 2026.

BRASIL. **Lei nº 14.155, de 27 de maio de 2021.** Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal). Brasília, DF: Presidência da República, 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm. Acesso em: 24 set. 2026.

BROCHADO, I. P. da S. **Investigação de crimes cibernéticos nas Polícias Civis do Brasil:** contribuição da gestão do conhecimento. 2025. 217 f. Dissertação (Mestrado em Engenharia e Gestão do Conhecimento) – Universidade Federal de Santa Catarina, Florianópolis, 2025. Disponível em: https://repositorio.ufsc.br/handle/123456789/265749. Acesso em: 24 set. 2026.

BUSTAMANTE, L. R.; SANTOS, L. R. F. dos; BATISTA, V. C. PIX: inovação financeira e suas consequências na economia brasileira. **Revista Foco,** v. 17, n. 12, e7292, 2024. DOI: 10.54751/revistafoco.v17n12-139. Disponível em: https://ojs.focopublicacoes.com.br/foco/article/view/7292. Acesso em: 24 set. 2026.

CAMPELO, T. L.; JAYME, F. R. A repercussão da internet no estelionato sentimental: uma perspectiva da vítima. **JNT – Facit Business and Technology Journal,** ed. 47, v. 2, p. 265-281, nov. 2023. Disponível em: https://revistas.faculdadefacit.edu.br/index.php/JNT/article/view/2667. Acesso em: 24 set. 2026.

CAPEZ, F. **Curso de direito penal:** parte especial (arts. 121 a 212). 25. ed. São Paulo: SaraivaJur, 2025. v. 2.

CARMO, A. S. S. do. O efeito da internet sobre o comércio internacional brasileiro: uma análise à luz do modelo gravitacional. **Revista Brasileira de Economia,** Rio de Janeiro, v. 76, n. 4, p. 490-511, 2022. DOI: 10.5935/0034-7140.20220021. Disponível em: https://periodicos.fgv.br/rbe/article/view/82307. Acesso em: 24 set. 2026.

CHOI, K. S.; LEE, C. S.; LOUDERBACK, E. R. Historical evolutions of cybercrime: from computer crime to cybercrime. In: HOLT, T. J.; BOSSLER, A. M. (ed.). **The Palgrave Handbook of International Cybercrime and Cyberdeviance.** Cham: Palgrave Macmillan, 2020. p. 27-43. DOI: 10.1007/978-3-319-78440-3_2. Disponível em: https://link.springer.com/referenceworkentry/10.1007/978-3-319-78440-3_2. Acesso em: 24 set. 2026.

CRESWELL, J. W.; CRESWELL, J. D. **Projeto de pesquisa:** métodos qualitativo, quantitativo e misto. 5. ed. Porto Alegre: Penso, 2021.

CUNHA, R. S. **Manual de direito penal:** parte especial (arts. 121 ao 361). 16. ed. Salvador: JusPodivm, 2023.

EVANGELISTA, A. J. S.; SILVA, H. H. B. Crimes cibernéticos: a relevância das alterações promovidas pela Lei 14.155/2021 no tocante aos crimes patrimoniais. **Lumen et Virtus,** São José dos Pinhais, v. 16, n. 47, p. 4409-4425, 2025. DOI: 10.56238/levv16n47-106. Disponível em: https://periodicos.newsciencepubl.com/LEV/article/view/4672. Acesso em: 24 set. 2026.

FBSP. Fórum Brasileiro de Segurança Pública. **Anuário Brasileiro de Segurança Pública.** 20. ed. São Paulo: FBSP, 2026. Disponível em: https://forumseguranca.org.br/wp-content/uploads/2026/07/anuario-2026.pdf. Acesso em: 24 set. 2026.

FEBRABAN. Federação Brasileira de Bancos. **Pesquisa Febraban de Tecnologia Bancária 2025.** São Paulo: Febraban, 2025. v. 1. Disponível em: https://cmsarquivos.febraban.org.br/Arquivos/documentos/PDF/Pesquisa%20Febraban%20de%20Tecnologia%20Banca%CC%81ria%202025%20-%20Vol_01%20-%205.pdf. Acesso em: 24 set. 2026.

FERREIRA, D. do N.; TEIXEIRA JÚNIOR, A. W. M. Categorizando atores não estatais violentos (ANEVs): o Novo Cangaço como um hibridismo criminal. **Revista Brasileira de Segurança Pública,** São Paulo, v. 19, n. 2, p. 182-199, 2025. DOI: 10.31060/rbsp.2025.v19.n2.2067. Disponível em: https://revista.forumseguranca.org.br/rbsp/article/view/2067. Acesso em: 24 set. 2026.

GASA. Global Anti-Scam Alliance; FEEDZAI. **Global State of Scams Report 2024.** Haia: GASA, 2024. Disponível em: https://www.feedzai.com/resource/global-state-of-scams-report-2024/. Acesso em: 24 set. 2026.

GIL, A. C. **Como elaborar projetos de pesquisa.** 7.Ed, Barueri: Atlas, 2022.

GOPINATH, M.; SETHURAMAN, S. C. A comprehensive survey on deep learning based malware detection techniques. **Computer Science Review,** v. 47, 100529, 2023. DOI: 10.1016/j.cosrev.2022.100529. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S1574013722000636. Acesso em: 24 set. 2026.

GRECO, R. **Código Penal comentado.** 17.ed., rev. e atual. São Paulo: Atlas, 2024.

HU, P.; BHUIYAN, M. A.; RAHMAN, M. K.; HOSSAIN, M. M.; AKTER, S. Impact of COVID-19 pandemic on consumer behavioural intention to purchase green products. **PLoS ONE,** v. 17, n. 10, e0275541, 2022. DOI: 10.1371/journal.pone.0275541. Disponível em: https://doi.org/10.1371/journal.pone.0275541. Acesso em: 24 set. 2026.

IBGE. Instituto Brasileiro de Geografia e Estatística. **Censo Demográfico 2022:** resultados da pesquisa. Rio de Janeiro: IBGE, 2023.

IBGE. Instituto Brasileiro de Geografia e Estatística. **Pesquisa Mensal de Comércio:** séries históricas – volume de vendas no comércio varejista ampliado. Rio de Janeiro: IBGE, 2026. Disponível em: https://www.ibge.gov.br/estatisticas/economicas/comercio/9227-pesquisa-mensal-de-comercio.html?edicao=45881&t=series-historicas. Acesso em: 21 set. 2026.

INTERPOL. **Global Financial Fraud Threat Assessment.** 2.ed., Lyon: INTERPOL, mar. 2026. Disponível em: https://www.interpol.int/content/download/24291/file/INTERPOLGlobalFinancialFraudThreatAssessment2026.pdf. Acesso em: 24 set. 2026.

IPEA. Instituto de Pesquisa Econômica Aplicada. **Anuário estatístico de segurança pública 2023-2024.** Brasília: Ipea, 2025. DOI: 10.38116/ri-anuario-estatistico-2023-2024. Disponível em: https://doi.org/10.38116/ri-anuario-estatistico-2023-2024. Acesso em: 24 set. 2026.

KUZIOR, A.; TIUTIUNYK, I.; ZIELIŃSKA, A.; KELEMEN, R. Cybersecurity and cybercrime: current trends and threats. **Journal of International Studies,** v. 17, n. 2, p. 220-239, 2024. DOI: 10.14254/2071-8330.2024/17-

2/12. Disponível em: https://doi.org/10.14254/2071-8330.2024/17-2/12. Acesso em: 24 set. 2026.

LEAL, R. G. Realidade virtual e criminalidade: tensões e desafios. **Revista de Direitos e Garantias Fundamentais,** Vitória, v. 24, n. 3, p. 107-135, set./dez. 2023. DOI: 10.18759/rdgf.v24i3.2304. Disponível em: https://sisbib.emnuvens.com.br/direitosegarantias/article/view/2304. Acesso em: 24 set. 2026.

MADARIE, R.; WEULEN KRANENBARG, M.; DE POOT, C. Cybersecurity expert perspectives on data thieves' actions in digital environments: potential refinements for routine activity theory. **Deviant Behavior,** 2025. DOI: 10.1080/01639625.2025.2453440. Disponível em: https://doi.org/10.1080/01639625.2025.2453440. Acesso em: 24 set. 2026.

MAGALHÃES, D. V. O Círio de Nazaré e o crescimento econômico local: um estudo sobre a maior manifestação religiosa católica. In: CONGRESSO NACIONAL DE ESTUDANTES E PROFISSIONAIS DE ADMINISTRAÇÃO (CONEPA), 13., 2025, Belém. **Anais [...].** Belém: CONEPA, 2025. Disponível em: https://doity.com.br/anais/belem2025/trabalho/466729. Acesso em: 21 set. 2026.

MARAGNO, R.; YAMAZATO, F. A. O estado de fraude e do estelionato digital no Brasil: evolução sistêmica, tipologias emergentes e a nova arquitetura de segurança (2020-2025). **Revista do Ministério Público Militar,** Brasília, v. 53, n. 50, p. 13-42, jan. 2026. DOI: 10.5281/zenodo.18175551. Disponível em: https://revista.mpm.mp.br/rmpm/article/view/512. Acesso em: 24 set. 2026.

MARCINEIRO, N.; WASSEM, L. A.; ORTMANN, A.; KNIES, R. A.; MEDEIROS DA COSTA, L. F. O problema dos dados do Boletim de Ocorrência para fins estatísticos. **Revista do Instituto Brasileiro de Segurança Pública,** v. 5, n. 13, p. 133-155, 2022. DOI: 10.36776/ribsp.v5i13.165. Disponível em: https://revista.ibsp.org.br/index.php/RIBSP/article/view/165. Acesso em: 24 set. 2026.

MARINHO, A. A.; FREITAS, A. G. T. de. **Manual de direito penal:** parte geral. 3.ed., São Paulo: Revista dos Tribunais, 2014.

MASSON, C. **Direito penal:** parte especial (arts. 121 a 212). 19. ed. rev., atual. e ampl. Rio de Janeiro: Método, 2026. v. 2.

NOVAIS, R. M. de; FARIA, A. H. P. de. Mudança no perfil do fenômeno criminal contra o patrimônio em Minas Gerais no período de 2018 a 2023: da prática violenta ao ambiente virtual. **Revista Brasileira de Segurança Pública,** São Paulo, v. 20, n. 1, p. 100-121, 2026. DOI: 10.31060/rbsp.2026.v20.n1.2071. Disponível em: https://doi.org/10.31060/rbsp.2026.v20.n1.2071. Acesso em: 24 set. 2026.

OLIVEIRA, A. P.; GOMES, D. Combate ao estelionato eletrônico no Brasil: análise das condições de investigação ocorridas no Pará, Piauí, Distrito Federal, São Paulo e Paraná. **Revista Brasileira de Criminalística,** v. 15, n. 1, p. 13-23, 2026. Disponível em: https://revista.rbc.org.br/index.php/rbc/article/view/955. Acesso em: 24 set. 2026.

OLIVEIRA, G. A. G.; ÁVILA, G. N. de. Deep fake, direitos da personalidade e o direito penal: uma análise dos impactos tecnológicos na era digital. **Revista Eletrônica do Curso de Direito**

da UFSM, Santa Maria, v. 19, e85239, p. 1-19, 2024. DOI: 10.5902/1981369485239. Disponível em: https://periodicos.ufsm.br/revistadireito/article/view/85239. Acesso em: 24 set. 2026.

PARK, I.; LEE, J.; LEE, D.; LEE, C.; CHUNG, W. Y. Changes in consumption patterns during the COVID-19 pandemic: analyzing the revenge spending motivations of different emotional groups. **Journal of Retailing and Consumer Services,** v. 65, 102874, 2022. DOI: 10.1016/j.jretconser.2021.102874. Disponível em: https://doi.org/10.1016/j.jretconser.2021.102874. Acesso em: 24 set. 2026.

PRADO, L. R. **Curso de direito penal brasileiro:** parte especial, arts. 121 a 249 CP. 24.ed., rev., ampl. e atual. São Paulo: Thoth, 2025. t. 1.

QUADROS, M. de; CRUZ, F. B. da. Desafios do direito penal na repressão da engenharia social em ambientes virtuais no Brasil. **Revista Internacional Consinter de Direito,** ano 10, n. 19, p. 413-427, 2024. DOI: 10.19135/revista.consinter.00019.18. Disponível em: https://revistaconsinter.com/index.php/ojs/article/view/446. Acesso em: 24 set. 2026.

RIBEIRO, G. A. M.; CORDEIRO, P. I. R. V.; FUMACH, D. M. O malware como meio de obtenção de prova e a sua implementação no ordenamento jurídico brasileiro. **Revista Brasileira de Direito Processual Penal,** Porto Alegre, v. 8, n. 3, p. 1463-1500, set./dez. 2022. DOI: 10.22197/rbdpp.v8i3.723. Disponível em: https://revista.ibraspp.com.br/RBDPP/article/view/723. Acesso em: 24 set. 2026.

SAMPAIO, H. A.; FERREIRA, A. B.; SECURATO, J. R. O impacto do PIX nos meios de pagamento no Brasil. **Revista Científica Hermes,** v. 37, n. 1, p. 44-59, 2025. DOI: 10.21710/rch.v37i1.769. Disponível em: https://doi.org/10.21710/rch.v37i1.769. Acesso em: 24 set. 2026.

SANTOS, J. F.; MIRANDA, W. D.; REIS NETTO, R. M. Engenharia social: o fator humano no incidente de segurança da informação. In: MIRANDA, W. D.; REIS NETTO, R. M.; REIS, J. F. G.; SANTOS, J. F. (org.). **Segurança pública e atividade de inteligência:** debates e perspectivas. Belém: Érgane, 2023. v. 2.

SANTOS, L. R. dos; SOTERO, A. P. da S. O estelionato virtual e a ineficácia da legislação brasileira para coibir o crime cibernético. **Cuadernos de Educación y Desarrollo,** v. 16, n. 8, e5183, 2024. DOI: 10.55905/cuadv16n8-081. Disponível em: https://ojs.cuadernoseducacion.com/ojs/index.php/ced/article/view/5183. Acesso em: 24 set. 2026.

SERASA EXPERIAN. Risco de fraude no e-commerce no Dia das Mães é 8,3% maior do que a média anual do setor; Serasa Experian alerta para cuidados na data. **Sala de Imprensa Serasa Experian,** São Paulo, 2025. Disponível em: https://www.serasaexperian.com.br/sala-de-imprensa/prevencao-a-fraude/risco-de-fraude-no-e-commerce-no-dia-das-maes-e-83-maior-do-que-a-media-anual-do-setor-serasa-experian-alerta-para-cuidados-na-data/. Acesso em: 30 jul. 2026.

SILVA, B. C. **Cybercrimes contra mulheres no Estado do Pará.** 2020. 125 f. Dissertação (Mestrado em Segurança Pública) – Programa de Pós-Graduação em Segurança Pública, Instituto de Filosofia e Ciências Humanas, Universidade Federal do Pará, Belém, 2020.

Disponível em: https://ppgsp.propesp.ufpa.br/ARQUIVOS/teses_e_dissertacoes/dissertacoes/2018/201815%20-%20SILVA.pdf. Acesso em: 24 set. 2026.

SILVA, S. S.; RAMOS, E. M. L. S.; REIS NETTO, R. M. Card - Elementos distintivos entre furto e estelionato eletrônico. Programa de Pós-Graduação em Segurança Pública. Instituto de Ciências Exatas e Naturais. Universidade Federal do Pará – PPGSP/ICEN/UFPA, 2026. Disponível em: http://educapes.capes.gov.br/handle/capes/1191955. Acesso em: 23.10.2026

SOUSA, G. E. A.; MAIA, B. G.; LIMA JÚNIOR, A. B.; MELLO, C. M. A.; SENA, R. R.; AUFIERO, M. J. M.; AGUIAR, K. R.; SIMAS, D. C. S. O impacto da inteligência artificial generativa na sofisticação de fraudes e golpes online com uso de deepfakes no Brasil. **Derecho y Cambio Social,** v. 22, n. 84, p. 1-23, 2025. DOI: 10.54899/dcs.v22i84.3604. Disponível em: https://doi.org/10.54899/dcs.v22i84.3604. Acesso em: 24 set. 2026.

STEINMETZ, K. F.; SCHAEFER, B. P.; MCCARTHY, A. L.; BREWER, C. G.; KURTZ, D. L. Exploring cybercrime capabilities: variations among cybercrime investigative units. **Criminal Justice Policy Review,** v. 35, n. 4, p. 194-215, 2024. DOI: 10.1177/08874034241265106. Disponível em: https://doi.org/10.1177/08874034241265106. Acesso em: 24 set. 2026.

SUXBERGER, A. H. G.; PACHECO, W. E. P. A teoria da anomia nos crimes cibernéticos. **Delictae:** Revista de Estudos Interdisciplinares sobre o Delito, v. 4, n. 7, p. 104-125, jul./dez. 2019. DOI: 10.24861/2526-5180.v4i7.105. Disponível em: https://delictae.com.br/index.php/revista/article/view/105. Acesso em: 24 set. 2026.

WILSON-KOVACS, D.; WILCOX, J. Managing policing demand for digital forensics through risk assessment and prioritization in England and Wales. **Policing: A Journal of Policy and Practice,** v. 17, paac106, 2023. DOI: 10.1093/police/paac106. Disponível em: https://doi.org/10.1093/police/paac106. Acesso em: 21 set. 2026.

WILSON, J. M.; GRAMMICH, C. A. Reframing the police staffing challenge: a systems approach to workforce planning and managing workload demand. **Policing: A Journal of Policy and Practice,** v. 18, paae005, 2024. DOI: 10.1093/police/paae005. Disponível em: https://doi.org/10.1093/police/paae005. Acesso em: 22 set. 2026.

---

[1] Mestranda do Programa de Pós-Graduação em Segurança Pública da Universidade Federal do Pará, Campus Belém. E-mail: acesse o artigo original para visualizar o e-mail

[2] Doutor em Engenharia de Produção (Universidade Federal de Santa Catarina - UFSC). Mestre em Estatística (Universidade Federal de Pernambuco - UFPE). Docente do Programa de Pós-Graduação em Segurança Pública (Universidade Federal do Pará - UFPA). E-mail: acesse o artigo original para visualizar o e-mail

[3] Doutor em Geografia (Universidade do Estado do Pará - UEPA). Mestre em Segurança Pública (Universidade Federal do Pará – UFPA) Docente do Programa de Pós-Graduação em Segurança Pública (Universidade Federal do Pará - UFPA). E-mail: acesse o artigo original para visualizar o e-mail