ReGeo ISSN: 2177-3246

QUEM SÃO AS VÍTIMAS DOS CRIMES PATRIMONIAIS PRATICADOS POR MEIO CIBERNÉTICO NO ESTADO DO PARÁ?

WHO ARE THE VICTIMS OF CYBER-ENABLED PROPERTY CRIMES IN THE STATE OF PARÁ, BRAZIL?

¿QUIÉNES SON LAS VÍCTIMAS DE LOS DELITOS CONTRA EL PATRIMONIO COMETIDOS POR MEDIOS CIBERNÉTICOS EN EL ESTADO DE PARÁ, BRASIL?

https://doi.org/10.56238/revgeov17n11-050

Data de submissão: 11/10/2026 **Data de publicação:** 11/11/2026

Shyrley Silva da Silva
Mestranda em Segurança Pública
Instituição: Universidade Federal do Pará (UFPA)
E-mail: shyrley.s.silva@gmail.com

Edson Marcos Leal Soares Ramos
Doutor em Engenharia de Produção
Instituição: Universidade Federal do Pará (UFPA)
E-mail: ramosedson@gmail.com

Roberto Magno Reis Netto
Doutor em Geografia
Instituição: Universidade Federal do Pará (UFPA)
E-mail: bob_reis_ufpa@yahoo.com.br

RESUMO

O artigo descreve o perfil sociodemográfico das vítimas de crimes patrimoniais praticados por meio cibernético registrados pela Polícia Civil do Pará de janeiro de 2022 a dezembro de 2025. Trata-se de pesquisa quantitativa, descritiva e documental, realizada sobre a totalidade dos 98.039 registros de boletins de ocorrência de estelionato praticado por meio eletrônico, fraude eletrônica e furto mediante fraude eletrônica, o que configura um censo. Sexo, idade, estado civil, profissão e escolaridade foram analisados por meio de distribuições de frequência e medidas descritivas. Os resultados indicam equilíbrio entre mulheres (51,45%) e homens (48,55%), média ponderada de 41,84 anos e moda de 28 anos, com 67,86% das vítimas de 20 a 49 anos e 15,80% com 60 anos ou mais. Predominam pessoas solteiras (46,78%) e com ensino médio completo (38,35%), e um quarto das vítimas tem ensino superior completo. Aposentados, estudantes, donas de casa e professores lideram as profissões informadas. Conclui-se que a vítima registrada não corresponde à imagem da pessoa pouco instruída, o que recomenda campanhas preventivas segmentadas e o aprimoramento do preenchimento dos boletins de ocorrência.

Palavras-chave: Perfil Sociodemográfico. Estelionato. Furto Mediante Fraude Eletrônica. Escolaridade. Boletins de Ocorrência.

ABSTRACT

This article describes the sociodemographic profile of victims of cyber-enabled property crimes recorded by the Civil Police of Pará from January 2022 to December 2025. It is a quantitative,

descriptive and documentary study covering all 98,039 police reports of swindling committed by electronic means, electronic fraud and theft by electronic fraud, which constitutes a census. Sex, age, marital status, occupation and education were analyzed through frequency distributions and descriptive measures. The results show a balance between women (51.45%) and men (48.55%), a weighted mean age of 41.84 years and a mode of 28 years, with 67.86% of victims aged 20 to 49 and 15.80% aged 60 or older. Single people (46.78%) and people with complete secondary education (38.35%) predominate, and one quarter of the victims have completed higher education. Retirees, students, homemakers and teachers lead the reported occupations. The registered victim does not match the image of a poorly educated person, which calls for segmented prevention campaigns and for better completion of police reports.

Keywords: Sociodemographic Profile. Swindling. Theft by Electronic Fraud. Education. Police Reports.

RESUMEN

El artículo describe el perfil sociodemográfico de las víctimas de delitos contra el patrimonio cometidos por medios cibernéticos registrados por la Policía Civil de Pará de enero de 2022 a diciembre de 2025. Se trata de una investigación cuantitativa, descriptiva y documental, realizada sobre la totalidad de las 98.039 denuncias policiales de estafa cometida por medios electrónicos, fraude electrónico y hurto mediante fraude electrónico, lo que configura un censo. El sexo, la edad, el estado civil, la profesión y la escolaridad se analizaron mediante distribuciones de frecuencia y medidas descriptivas. Los resultados indican equilibrio entre mujeres (51,45%) y hombres (48,55%), media ponderada de 41,84 años y moda de 28 años, con el 67,86% de las víctimas de 20 a 49 años y el 15,80% con 60 años o más. Predominan las personas solteras (46,78%) y con enseñanza secundaria completa (38,35%), y una cuarta parte de las víctimas tiene educación superior completa. Jubilados, estudiantes, amas de casa y profesores encabezan las profesiones informadas. La víctima registrada no corresponde a la imagen de una persona con poca instrucción, lo que recomienda campañas preventivas segmentadas y una mejor cumplimentación de las denuncias policiales.

Palabras clave: Perfil Sociodemográfico. Estafa. Hurto Mediante Fraude Electrónico. Escolaridad. Denuncias Policiales.

1 INTRODUÇÃO

A criminalidade patrimonial brasileira mudou de endereço nos últimos anos. Delitos que antes dependiam do encontro físico entre autor e vítima passaram a ser executados a distância, com o auxílio de aparelhos conectados, aplicativos de mensagens e sistemas de pagamento instantâneo, dinâmica que estudos recentes descrevem como a passagem da prática violenta para o ambiente virtual e como uma verdadeira industrialização do estelionato (Novais; Faria, 2026; Maragno; Yamazato, 2026).

A escala do fenômeno ajuda a compreender a preocupação que ele desperta. A Interpol (2026) estimou em 442 bilhões de dólares as perdas globais com fraudes financeiras em 2025. No plano interno, o Anuário Brasileiro de Segurança Pública contabilizou 2.261.055 ocorrências de estelionato no país em 2025, o que corresponde a cerca de 4,3 registros por minuto (FBSP, 2026).

Parte dessa expansão acompanha a velocidade com que a vida financeira se digitalizou no país. O Pix, lançado em novembro de 2020, reduziu o uso de instrumentos tradicionais, como boletos e transferências bancárias convencionais (Bustamante; Santos; Batista, 2024; Sampaio; Ferreira; Securato, 2025), e chegou ao fim de 2025 com 148,13 milhões de pessoas físicas usuárias, perto de 86% da população adulta. O próprio Banco Central observa que essa ampla adoção veio acompanhada do uso crescente do Pix como meio de distribuição de fraudes, golpes e ataques a instituições participantes (BCB, 2026).

No campo legislativo, a Lei Nº 14.155, de 27 de maio de 2021 (Brasil, 2021), criou formas qualificadas para o furto mediante fraude eletrônica e para o estelionato cometido por meio eletrônico, mudança cuja relevância para os crimes patrimoniais praticados pela internet é destacada pela literatura (Evangelista; Silva, 2025). No furto mediante fraude eletrônica, a lei também previu aumento de pena quando a vítima é idosa ou vulnerável, sem, contudo, definir o que se deve entender por vulnerabilidade tecnológica (Lai; Mourão, 2021).

Se a evolução dos tipos penais e das estatísticas de ocorrência recebeu atenção crescente, o mesmo não se pode dizer de quem sofre o dano. O país ainda não conta com pesquisas de vitimização periódicas, nem com um programa nacional cujas amostras permitam análises por estado ou município (FBSP; Datafolha, 2025). Pesquisadores da área também recomendam análises aprofundadas de dados forenses e de investigações criminais para medir o avanço da criminalidade digital no Brasil (Sousa *et al.*, 2025), e a lacuna pesa ainda mais porque o consumidor que atua no ambiente virtual tende a ser mais vulnerável, já que muitas vezes lhe faltam informação e preparo técnico para as operações feitas pela internet (Lehfeld *et al.*, 2021).

As consequências para quem é lesado vão além do valor perdido. Fraudes e golpes eletrônicos produzem efeitos difíceis de mensurar, que extrapolam o prejuízo econômico imediato e incluem

abalos psicológicos e instabilidade econômica (Siqueira, 2024), e, nos golpes sentimentais praticados pela internet, as vítimas relatam, além da perda de dinheiro, decepção emocional e traumas psicológicos (Campelo; Jayme, 2023). Conhecer quem são essas pessoas é, portanto, condição para dimensionar o problema e para desenhar respostas que alcancem quem de fato está sendo atingido.

No Pará, o tema ganha contornos próprios. O estado registrou, no período de 2024 a 2025, crescimento do estelionato por meio eletrônico superior à média nacional (FBSP, 2026). Pesquisas desenvolvidas no âmbito do Programa de Pós-Graduação em Segurança Pública da Universidade Federal do Pará (PPGSP/UFPA) já evidenciaram o peso do estelionato entre os cibercrimes contra mulheres (Silva, 2020) e examinaram o golpe afetivo conhecido como *romance scam* (Souza, 2022), o que revela o interesse local pelo tema e abre espaço para uma caracterização mais ampla das vítimas registradas no estado.

Diante desse quadro, o objetivo deste artigo é descrever quem são as vítimas dos crimes patrimoniais praticados por meio cibernético que constam dos registros da Polícia Civil do estado do Pará no período de 2022 a 2025, segundo sexo, idade, estado civil, profissão e escolaridade. Ao deslocar o olhar do autor e do tipo penal para a pessoa lesada, o estudo procura oferecer subsídios para ações preventivas mais bem direcionadas e para o aprimoramento dos registros policiais.

O texto está organizado em cinco seções, incluindo esta introdução. A segunda reúne o referencial teórico sobre os tipos penais envolvidos e a posição da vítima, a engenharia social e o registro das ocorrências. A terceira descreve o percurso metodológico, a quarta apresenta e discute os resultados e a quinta reúne as conclusões.

2 REFERENCIAL TEÓRICO

2.1 A VÍTIMA NOS CRIMES PATRIMONIAIS PRATICADOS POR MEIO CIBERNÉTICO

Os crimes contra o patrimônio são crimes comuns, de modo que qualquer pessoa, física ou jurídica, pode figurar como sujeito passivo, desde que certa e identificável (Greco, 2025; Nucci, 2025). No ambiente digital, a resposta específica do legislador para os delitos patrimoniais concentra-se em dois tipos penais, o furto mediante fraude eletrônica e o estelionato eletrônico, que a lei denomina fraude eletrônica (Brasil, 1940; Evangelista; Silva, 2025).

O que diferencia as duas figuras é o papel desempenhado pela vítima. No furto mediante fraude eletrônica, o bem é retirado sem que o titular perceba, com o uso de aparelho eletrônico ou informático, conectado ou não à internet, haja ou não violação de mecanismo de segurança ou emprego de programa malicioso (Lai; Mourão, 2021; Cunha, 2023). No estelionato eletrônico, ao contrário, o engano alcança a formação da vontade, e é a própria vítima que, levada a uma falsa percepção da realidade, entrega o

bem ou a vantagem ao agente (Prado, 2025; Masson, 2026). Mensagens que prometem prêmios inexistentes, *links* falsos e ligações dirigidas a pessoas vulneráveis, sobretudo idosas, aparecem na doutrina como exemplos típicos do estelionato eletrônico (Greco, 2024; Capez, 2025).

O tratamento penal dessas condutas ficou mais rigoroso em 2026. A Lei Nº 15.397, de 30 de abril de 2026 (Brasil, 2026), elevou a pena do furto mediante fraude eletrônica para reclusão de 4 a 10 anos e manteve em 4 a 8 anos a do estelionato eletrônico, que se configura quando o agente se vale de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou mensagens de correio eletrônico fraudulentas, lista à qual a nova lei acrescentou a duplicação de dispositivo eletrônico ou de aplicação de internet.

A mesma lei revogou o dispositivo que exigia a representação da vítima para o processamento do estelionato, de modo que o crime voltou a ser, como regra, de ação penal pública incondicionada, alteração que não alcança os fatos anteriores à sua vigência por ser mais gravosa ao acusado (FBSP, 2026). Para a vítima, a mudança significa que a persecução penal deixa de depender de sua manifestação formal, embora continue dependendo, em grande medida, de que o fato chegue ao conhecimento da polícia.

A posição da vítima também influencia o lugar em que o caso será processado. No furto mediante fraude eletrônica, vale a regra geral do Código de Processo Penal (Brasil, 1941), que, em princípio, fixa a competência no local em que o crime se consuma (Lima, 2026). No estelionato praticado mediante depósito, transferência de valores ou emissão de cheque sem fundos, a Lei Nº 14.155/2021, que alterou o Código Penal (Brasil, 1940), passou a fixar a competência pelo domicílio da vítima e, havendo várias vítimas, pela prevenção (Lopes Jr., 2026). A regra aproxima a persecução penal do lugar onde vive quem foi lesado, o que reforça a utilidade de conhecer o perfil das vítimas em cada unidade da Federação.

Para avaliar se o meio fraudulento era capaz de enganar, a doutrina costuma tomar como parâmetro o homem médio, ou seja, alguém comum, sem formação técnica ou jurídica específica, e só em situações excepcionais leva em conta a fragilidade particular de quem foi enganado (Greco, 2024; Nucci, 2025).

No caso das pessoas idosas, a literatura descreve uma hipervulnerabilidade diante das fraudes bancárias eletrônicas, associada a limitações técnicas e ao declínio das capacidades funcionais que acompanha o envelhecimento (Volpato; Pegoraro Junior, 2024). Essa condição se soma à vulnerabilidade do consumidor no ambiente digital, que muitas vezes nem sabe que seus dados pessoais são recolhidos de forma contínua e sem aviso (Lehfeld *et al.*, 2021).

2.2 ENGENHARIA SOCIAL E EXPOSIÇÃO AO RISCO

O elemento comum às diferentes modalidades de golpes é a engenharia social, entendida como um conjunto de práticas que se valem da manipulação, do convencimento e da influência sobre a vítima para obter dela informações valiosas (Quadros; Cruz, 2024). A Agência Brasileira de Inteligência a descreve como uma forma de ataque que dispensa a força física e se apoia no engano e na confiança alheia, para que a própria pessoa tome decisões que a prejudicam, como revelar dados sigilosos ou enviar dinheiro a desconhecidos (ABIN, 2021).

Para Hatfield (2018), o conceito se sustenta em três elementos. O primeiro é a assimetria epistemológica, que existe quando uma das partes sabe muito mais do que a outra sobre determinado assunto; o segundo é a dominância tecnocrática, que transforma essa vantagem em instrumento de influência; e o terceiro é a substituição teleológica, pela qual o agente desvia o comportamento do alvo para servir aos próprios objetivos. Santos, Miranda e Reis Netto (2023) acrescentam que essas técnicas exploram a propensão cognitiva da pessoa, um desvio de julgamento que a leva a acreditar que está decidindo corretamente ao atender ao pedido de quem a engana.

A sofisticação desses expedientes tende a aumentar. Os conteúdos audiovisuais sintéticos, conhecidos como *deepfakes*, imitam o rosto, os gestos e a voz de pessoas reais com um realismo que torna difícil diferenciá-los de gravações autênticas (Oliveira; Ávila, 2024). As ferramentas de inteligência artificial generativa, por sua vez, exigem menos trabalho e expõem menos o fraudador, o que facilita o golpe, permite reproduzi-lo em larga escala e dificulta sua detecção logo no início, com usos que vão da redação automática de grande volume de mensagens de *phishing* verossímeis à clonagem de voz e à manipulação do rosto para que o criminoso se passe por outra pessoa (Sousa *et al.*, 2025).

Quando o engano fica tecnicamente mais refinado, a proteção deixa de depender apenas da atenção individual. Em experimento pré-registrado, os participantes não conseguiram identificar com segurança vídeos falsificados por inteligência artificial (Köbis; Doležalová; Soraperra, 2021). A ideia de que somente pessoas pouco informadas caem em golpes também perde força, já que estudo com amostra representativa da população holandesa não encontrou um perfil claro de quem corre mais risco de fraude e verificou que a escolaridade mais alta esteve associada a maior exposição a vários tipos de fraude, como as de investimento e de prêmios e o *phishing* (Koning; Junger; Veldkamp, 2024).

Do lado dos autores, os grupos que atuam *on-line* tendem a dispensar hierarquias formais e a funcionar em redes e alianças passageiras, que não se limitam a fronteiras nacionais nem a diferenças culturais (Leal, 2023), configuração que, no Brasil, assume feição de escala industrial, com divisão de tarefas, roteiros padronizados e metas de arrecadação (FBSP, 2026). Uma hipótese é a de que essa

escala amplie o contato com um grande número de pessoas, de modo que o perfil das vítimas registradas reflita, em boa medida, a composição de quem é alcançado pelo contato criminoso, e não apenas características individuais de quem é enganado.

2.3 REGISTRO, SUBNOTIFICAÇÃO E QUALIDADE DA INFORMAÇÃO

Toda análise baseada em boletins de ocorrência descreve, antes de tudo, as vítimas que procuraram a polícia. O boletim registra o crime que chegou ao conhecimento policial, e não todo crime praticado, por isso fica difícil saber se uma alta ou uma queda nos números expressa mudança real do fenômeno ou apenas variação no volume de comunicações (Almeida *et al.*, 2023). Nos golpes sentimentais, a vergonha e o medo levam muitas vítimas a evitar a exposição pública do que viveram, o que engrossa a cifra oculta desses delitos (Campelo; Jayme, 2023), e é plausível supor que algo semelhante ocorra em outras modalidades de golpe.

A baixa responsabilização dos autores também pode pesar na decisão de registrar. No mesmo ano em que o país somou mais de 2,2 milhões de registros de estelionato, foram contabilizados 63.771 processos penais e 4.819 presos por esse crime (FBSP, 2026). Pesquisa com profissionais da investigação criminal cibernética registra frustrações com a falta de efetividade das normas, a ausência de procedimentos uniformes e a estrutura insuficiente (Wendt, 2024). Para quem foi lesado, a percepção de que o registro raramente leva à punição pode reduzir o incentivo para procurar a polícia, sobretudo quando o valor perdido é pequeno.

A qualidade da informação registrada é outra preocupação. Os dados do boletim de ocorrência têm limitações para uso estatístico, porque muitas vezes são lançados de forma incorreta e sem o devido cuidado com sua qualidade (Marcineiro *et al.*, 2022), e cada polícia civil define os próprios procedimentos de registro, o que compromete a padronização e a comparabilidade dos dados no país (Ipea, 2025). Para o estudo do perfil das vítimas, essas limitações pesam diretamente, já que variáveis como escolaridade e profissão dependem do cuidado de quem faz o registro e, provavelmente, do que a pessoa declara no atendimento.

Conhecer quem são as vítimas registradas tem, por isso, valor duplo. Serve para orientar a prevenção, já que especialistas ouvidos em pesquisa sobre a evolução do *phishing* apontam a educação do público e a adoção de hábitos de segurança, ao lado de ferramentas automatizadas de detecção, como caminhos para conter esse tipo de golpe (Ghazi-Tehrani; Pontell, 2021). Serve também para aproximar a segurança pública de uma atuação centrada na vítima, orientação que estudo com registros de cerca de 380 mil vítimas da polícia de Kent, no Reino Unido, associa a uma atividade policial mais eficiente, sobretudo na prevenção (Lay; Ariel; Harinam, 2023).

3 METODOLOGIA

A pesquisa adota abordagem quantitativa, voltada à mensuração e à comparação de variáveis (Creswell; Creswell, 2021), e tem caráter descritivo e exploratório, pois busca detalhar as características de um fenômeno e levantar hipóteses para investigações futuras (Gil, 2022). Quanto aos procedimentos, combina pesquisa bibliográfica, construída a partir da produção já publicada por outros autores em livros, artigos, dissertações e relatórios institucionais (Sousa; Oliveira; Alves, 2021), e pesquisa documental, realizada sobre boletins de ocorrência entregues já sistematizados em planilha eletrônica.

O estudo tem como lócus o estado do Pará, na região Norte do Brasil, segunda maior unidade da Federação em extensão territorial, com cerca de 14,6% do território nacional, 144 municípios e 8.120.131 habitantes no Censo Demográfico de 2022 (IBGE, 2023a).

Os registros foram cedidos pela Secretaria Adjunta de Inteligência e Análise Criminal (SIAC), órgão da Secretaria de Estado de Segurança Pública e Defesa Social do Pará, e extraídos do Sistema Integrado de Segurança Pública (SISP), no qual a Polícia Civil do estado lança suas ocorrências e procedimentos.

A base reúne 98.039 registros de boletins de ocorrência lavrados de janeiro de 2022 a dezembro de 2025 e abrange três enquadramentos do Código Penal (Brasil, 1940), que são o estelionato na forma simples com indicação de que foi praticado por meio eletrônico, o estelionato eletrônico, previsto no § 2º-A do Art. 171 e chamado pelo legislador de fraude eletrônica, e o furto mediante fraude eletrônica, previsto no § 4º-B do Art. 155. Como todos os registros foram analisados, a pesquisa configura um censo, sem necessidade de amostragem nem de cálculo de erro amostral. O recorte começa em 2022 porque as formas qualificadas foram criadas pela Lei Nº 14.155/2021 (Brasil, 2021), publicada em maio daquele ano, de modo que o período analisado cobre apenas anos completos de vigência das novas figuras penais.

A unidade de análise é o registro, e não a pessoa. Cada registro traz os atributos de uma vítima vinculada a uma ocorrência, de forma que alguém que tenha registrado mais de um boletim no período aparece mais de uma vez na base. As vítimas pessoas jurídicas foram excluídas das distribuições, assim como os registros sem informação em cada variável, razão pela qual as bases de cálculo variam conforme o atributo analisado, como mostra o Quadro 1. Na profissão, a exclusão recaiu sobre os registros lançados na categoria genérica “outras profissões”.

Quadro 1. Variáveis do perfil das vítimas, categorias e quantidade de registros válidos e excluídos de estelionato por meio eletrônico, fraude eletrônica e furto mediante fraude eletrônica, no período de janeiro de 2022 a dezembro de 2025.

Variável	Categorias	Registros válidos	Registros excluídos[1]
Sexo	Feminino; masculino	97.421	618
Faixa de idade	0 a 11 anos; 12 a 17; 18 a 19; 20 a 29; 30 a 39; 40 a 49; 50 a 59; 60 anos ou mais	97.146	893
Idade em anos	Média simples das idades distintas, média ponderada pelas vítimas, moda e ponto médio da amplitude	97.120	919
Estado civil	Solteiro(a); casado(a); união estável; divorciado(a); viúvo(a)	96.431	1.608
Escolaridade	Não alfabetizado; fundamental incompleto; fundamental completo; médio incompleto; médio completo; superior incompleto; superior completo	95.633	2.406
Profissão	Vinte profissões mais frequentes	81.374	16.665

Notas: [1] Pessoas jurídicas e registros sem informação na variável; na profissão, registros lançados na categoria genérica "outras profissões".
Fonte: Elaborado pelos autores

A planilha enviada pela SIAC passou, primeiro, pela conferência do período de referência e do total de registros e, em seguida, por tratamento no Microsoft Excel, que uniformizou a nomenclatura das categorias, ajustou campos inconsistentes, verificou duplicidades e confirmou os totais. Foram mantidas as ocorrências consumadas e as tentadas, já que em ambas há uma pessoa visada pela ação criminosa. Do conjunto de campos disponíveis, extraíram-se apenas os relativos à vítima, isto é, sexo, idade em anos, faixa de idade, estado civil, escolaridade e profissão, que foram tabulados em frequências absolutas e relativas e deram origem às tabelas e aos gráficos da seção de resultados.

Como produto dessa etapa, a tabulação gerou duas distribuições percentuais, relativas ao sexo e à escolaridade das vítimas, apresentadas em gráficos, e quatro tabelas, que reúnem a distribuição por faixa de idade, o resumo estatístico das idades, a distribuição por estado civil e as vinte profissões mais frequentes. Esses seis elementos constituem a base empírica analisada na seção de resultados. As faixas etárias seguem a classificação da base, que reúne crianças de 0 a 11 anos, adolescentes de 12 a 17 anos, jovens adultos de 18 a 19 anos, quatro faixas decenais de 20 a 59 anos e pessoas com 60 anos ou mais, corte que coincide com o do Estatuto da Pessoa Idosa (Brasil, 2003).

Os dados foram analisados quantitativamente, por meio da contagem de registros em cada categoria das variáveis da vítima, do cálculo dos respectivos percentuais e de medidas-resumo da idade, dispostos em tabelas e gráficos que permitem comparar os grupos e identificar onde os registros se concentram (Bussab; Morettin, 2023). Os percentuais correspondem à razão entre o número de registros de cada categoria e o total de registros válidos da variável, informado no Quadro 1.

Para a idade, foram calculadas quatro medidas, cada uma com finalidade própria. Na média simples, somaram-se as 108 idades distintas registradas, de 0 a 125 anos, e o resultado foi dividido por

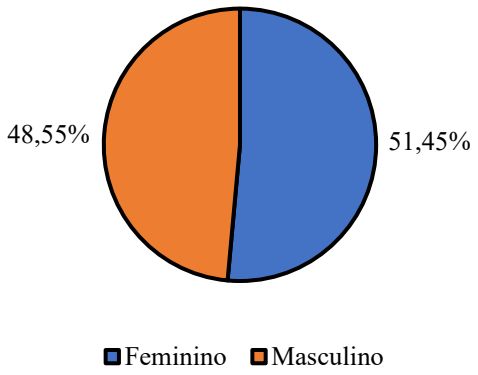
108, o que deu 54,28 anos, valor que considera cada idade uma única vez, sem levar em conta quantas vítimas possuem cada idade. Na média ponderada, cada idade foi multiplicada pelo respectivo número de vítimas, os produtos foram somados e o resultado foi dividido pelo total de 97.120 vítimas com idade informada, chegando-se a 41,84 anos, média que melhor representa as vítimas. A moda foi identificada pela comparação dos quantitativos de vítimas de todas as idades, e a de 28 anos apresentou a maior frequência, com 2.578 vítimas. O ponto médio resulta da soma da menor idade observada, 0 ano, com a maior, 125 anos, dividida por dois, dando o resultado de 62,50 anos, valor que representa apenas o centro da amplitude observada.

4 RESULTADOS E DISCUSSÃO

4.1 SEXO

A Figura 1 apresenta, em gráfico de setores, a distribuição percentual das vítimas segundo o sexo registrado no boletim de ocorrência, tomando como base os registros em que essa informação consta, o que permite comparar a participação de mulheres e homens no total de vítimas de crimes patrimoniais praticados por meio cibernético no estado.

Gráfico 1. Percentual de vítimas de crimes patrimoniais praticados por meio cibernético, no estado do Pará no período de 2022 a 2025, por sexo.



Fonte: Elaborado pelos autores a partir de dados do SIAC, setembro/2026.

A distribuição entre os sexos é praticamente equilibrada. Dos 97.421 registros com essa informação, 50.124 (51,45%) referem-se a mulheres e 47.297 (48,55%) a homens, diferença de apenas 2,90 pontos percentuais, ou 2.827 registros, ao longo de quatro anos. Os 618 registros excluídos, que equivalem a 0,63% da base, correspondem a pessoas jurídicas ou a ocorrências sem essa informação.

A leve predominância feminina não autoriza afirmar que as mulheres sejam alvo preferencial desses crimes. Uma diferença inferior a três pontos percentuais, em uma base de quase cem mil

registros, indica distribuição muito próxima da paridade, o que sugere que o sexo, isoladamente, pouco explica quem se torna vítima.

Pesquisas realizadas nos Estados Unidos e no Canadá também não indicam um padrão único associado ao sexo, pois mostram que o peso do gênero entre os fatores de risco varia conforme o tipo de golpe (DeLiema; Li; Mottola, 2023) e que os fatores associados à fraude on-line diferem entre homens e mulheres (Maher *et al.*, 2026).

Uma hipótese compatível com esse equilíbrio é a de que a exposição esteja mais ligada ao uso cotidiano de contas digitais, aplicativos bancários e do Pix, hoje utilizado por cerca de 86% da população adulta brasileira (BCB, 2026), do que a características associadas ao sexo. Outra hipótese é a de que homens e mulheres sejam abordados por golpes diferentes, ainda que em volumes semelhantes, possibilidade que encontra respaldo em pesquisa com amostra representativa da população holandesa, na qual não houve diferença entre os sexos na vitimização por fraude, mas os homens se mostraram mais expostos às fraudes de investimento, de prêmios, de doações e de relacionamento e ao *phishing*, e menos suscetíveis às fraudes em compras (Koning; Junger; Veldkamp, 2024).

A comparação com a composição da população reforça essa leitura, pois, segundo o Censo Demográfico de 2022, as mulheres correspondem a 50,10% dos 8.120.131 residentes no Pará (IBGE, 2023b), proporção apenas 1,35 ponto percentual abaixo de sua participação entre as vítimas. Relacionando os registros à população de cada sexo, obtêm-se cerca de 1.232 vítimas por 100 mil mulheres e 1.167 por 100 mil homens no acumulado de 2022 a 2025, razão de aproximadamente 1,06. O acesso à internet, condição para a exposição a esses crimes, também se distribui de modo semelhante, já que, segundo a pesquisa TIC Domicílios 2024, 85% dos homens e 84% das mulheres no Brasil haviam usado a rede nos três meses anteriores à entrevista, e 96% dos usuários de ambos os sexos a acessavam todos os dias ou quase todos os dias (CGI.br, 2025a).

4.2 IDADE

A Tabela 1 apresenta o quantitativo e o percentual de vítimas de crimes patrimoniais praticados por meio cibernético distribuídos em oito faixas de idade, segundo a idade registrada no boletim de ocorrência, tomando como base os 97.146 registros em que essa informação consta e permitindo identificar em quais etapas da vida as vítimas se concentram.

Tabela 1. Quantitativo e percentual de vítimas de crimes patrimoniais praticados por meio cibernético, por faixa de idade, no estado do Pará no período de 2022 a 2025.

Faixa de idade	Quantitativo	Porcentagem
0 a 11 anos	106	0,11%
12 a 17 anos	160	0,16%
18 a 19 anos	2.122	2,18%
20 a 29 anos	22.323	22,98%
30 a 39 anos	23.677	24,37%
40 a 49 anos	19.925	20,51%
50 a 59 anos	13.480	13,88%
60 anos ou mais	15.353	15,80%
Total	**97.146**	**100,00%**

Fonte: Elaborado pelos autores a partir de dados do SIAC, setembro/2026.

A faixa de 30 a 39 anos reúne o maior número de vítimas, com 23.677 registros (24,37%), seguida pelas faixas de 20 a 29 anos, com 22.323 (22,98%), e de 40 a 49 anos, com 19.925 (20,51%). Juntas, essas três faixas concentram 65.925 registros, o equivalente a 67,86% do total. Na sequência aparecem as pessoas com 60 anos ou mais, com 15.353 registros (15,80%), e as de 50 a 59 anos, com 13.480 (13,88%). As faixas iniciais têm participação reduzida, pois os jovens de 18 a 19 anos somam 2.122 registros (2,18%), e crianças e adolescentes, juntos, 266 registros (0,27%).

A frequência acumulada mostra que 49,81% das vítimas têm até 39 anos e que 70,32% têm até 49 anos, o que situa a mediana no início da faixa de 40 a 49 anos. Como as faixas de 20 a 59 anos têm a mesma amplitude, elas podem ser comparadas diretamente, e a comparação mostra que a participação cresce até a faixa de 30 a 39 anos e diminui a partir dela, com queda mais acentuada depois dos 50 anos.

A faixa de 18 a 19 anos, composta por jovens adultos, abrange apenas dois anos de idade, enquanto as faixas de 20 a 59 anos abrangem dez anos cada, o que impede compará-las pelo total de registros e exige que a análise seja feita por ano de idade. Por esse critério, a faixa de 18 a 19 anos reúne cerca de 1.061 registros por ano de idade, ao passo que as de 20 a 29 e de 30 a 39 anos reúnem cerca de 2.232 e 2.368, respectivamente, mais que o dobro.

Uma hipótese para a maior concentração de registros de 20 a 49 anos é a de que ela acompanhe a maior inserção dessas pessoas no mercado de trabalho e na rotina bancária digital, o que envolve movimentar contas, receber salários e realizar pagamentos e transferências com frequência, ampliando as oportunidades de contato com os criminosos.

Esse padrão é compatível com dados de outros países. Na União Europeia, a faixa de 25 a 39 anos foi a mais atingida por fraudes on-line ao longo da vida, com 30% de vítimas, contra 19% entre as pessoas com 55 anos ou mais (FRA, 2026), e, nos Estados Unidos, as pessoas de 18 a 59 anos

tiveram probabilidade 34% maior de relatar perda de dinheiro com fraudes do que as de 60 anos ou mais (FTC, 2022). A relação com a vida profissional também aparece na literatura, pois, em amostra representativa de adultos norte-americanos, os mais jovens com rotinas de trabalho ligadas ao computador foram mais vitimados do que os mais velhos com rotinas semelhantes (Parti, 2023), e, na Austrália, a proporção de vítimas de fraudes e golpes *on-line* foi maior entre desempregados (9,2%) e empregados (8,3%) do que no grupo formado por aposentados, estudantes, donas de casa e outras pessoas que não trabalhavam (6,7%) (Voce; Morgan, 2023).

Os 266 registros envolvendo crianças e adolescentes admitem mais de uma explicação. A primeira é a de vitimização efetiva, possibilidade compatível com pesquisa realizada na Dinamarca, em que 36% das crianças e adolescentes que negociavam itens virtuais ou contas de jogos disseram já ter sofrido golpe nessas trocas (Kristiansen; Jensen, 2023). No Brasil, esse público também já movimenta dinheiro na internet, pois, na pesquisa TIC Kids Online Brasil 2025, que ouviu 2.370 crianças e adolescentes de 9 a 17 anos usuários da rede, 21% dos que tinham de 11 a 17 anos relataram ter feito alguma compra ou gasto para avançar de fase ou obter itens novos em jogos on-line, proporção que chega a 24% entre os de 15 a 17 anos (CGI.br, 2025b).

A segunda é a de que esses casos envolvam o uso de dados, contas ou aparelhos de pessoas menores de idade, o que a literatura internacional chama de fraude de identidade infantil, situação em que a identidade da criança é usada para abrir contas em seu nome sem autorização e que, segundo pesquisa norte-americana, atinge uma em cada 50 crianças por ano, sendo que cerca de três em cada quatro vítimas conhecem pessoalmente o autor (Javelin Strategy & Research, 2021). A terceira é a de erro no preenchimento da data de nascimento, possibilidade coerente com os problemas já apontados no uso estatístico dos boletins de ocorrência (Marcineiro *et al.*, 2022).

As pessoas com 60 anos ou mais somam 15.353 registros, o que significa que cerca de uma em cada seis vítimas registradas é idosa, segundo o critério do Estatuto da Pessoa Idosa (Brasil, 2003), resultado que converge com a liderança dos aposentados entre as profissões (Tabela 4), analisada adiante. Essa participação ganha relevo quando se considera que, em pesquisas de vitimização de outros países, a ocorrência de crimes cibernéticos tende a diminuir com a idade, como na Inglaterra e no País de Gales, onde atingiu 9,13% dos usuários de internet de 16 a 24 anos e 2,66% dos com 75 anos ou mais, embora estes tenham apresentado maior probabilidade de relatar perda financeira quando vitimados (Havers *et al.*, 2024).

A literatura associa a hipervulnerabilidade desse público à grande dificuldade de lidar com novas tecnologias e à frequente dependência da ajuda de familiares, fatores que o expõem a golpes de engenharia social como o da falsa central, apontado como muito comum entre pessoas idosas (Volpato;

Pegoraro Junior, 2024), além da maior confiança em figuras de autoridade e da menor familiaridade com a linguagem de segurança *on-line* (Burton *et al.*, 2022).

Embora expressivo, esse contingente pode estar subestimado, pois pessoas idosas podem deixar de revelar a vitimização por vergonha, constrangimento ou receio de não serem levadas a sério (Burton *et al.*, 2022; Havers *et al.*, 2024), e, em amostra representativa de adultos norte-americanos, 64,10% das vítimas idosas de fraude on-line não procuraram ninguém para relatar o golpe, contra 14,00% das mais jovens (Parti, 2023).

A preocupação com esse público também chegou ao Legislativo. Tramita na Câmara dos Deputados o Projeto de Lei Nº 3.332/2025, que dispõe sobre a proteção de pessoas idosas contra fraudes financeiras em instituições financeiras e foi aprovado, com emenda, pela Comissão de Defesa dos Direitos da Pessoa Idosa em outubro de 2025, mas ainda segue em tramitação (Brasil, 2025).

A Tabela 2 reúne, para o conjunto de vítimas com idade informada, as medidas que resumem a distribuição dessas idades. A média simples corresponde à média aritmética das idades distintas observadas, sem ponderar pelo número de vítimas em cada uma, e a média ponderada leva em conta quantas vítimas têm cada idade, motivo pelo qual as duas apresentam valores tão diferentes. A moda indica a idade que mais se repete entre as vítimas, e o ponto médio da amplitude corresponde ao valor central entre a menor e a maior idade registradas na base.

Tabela 2. Quantitativo de vítimas com idade informada e resumo estatístico das idades das vítimas de crimes patrimoniais praticados por meio cibernético, no estado do Pará no período de 2022 a 2025.

Medida	**Resultado**
Média simples das idades distintas	54,28 anos
Média ponderada pelas vítimas	41,84 anos
Moda	28,00 anos
Ponto médio da amplitude	62,50 anos
Vítimas com idade informada	97.120

Fonte: Elaborado pelos autores a partir de dados do SIAC, setembro/2026.

A média ponderada pelas vítimas, de 41,84 anos, é a medida que melhor resume a idade de quem registrou a ocorrência, porque considera quantas vítimas há em cada idade. Ela se situa logo acima do limite inferior da faixa de 40 a 49 anos e próxima da mediana, que, como visto, está no início dessa faixa. A moda, de 28 anos, foi a idade isolada mais frequente, com 2.578 vítimas, e pertence à faixa de 20 a 29 anos.

A média simples das idades distintas, de 54,28 anos, deve ser lida de outra forma. Por considerar cada uma das 108 idades presentes na base uma única vez, independentemente do número de vítimas, ela descreve a amplitude das idades registradas, e não o perfil de quem foi lesado. A diferença de 12,44

anos em relação à média ponderada mostra que as idades mais altas aparecem na base, mas com poucas vítimas, enquanto a maior parte dos registros se concentra em idades bem mais baixas.

O ponto médio da amplitude, de 62,50 anos, resulta da menor idade registrada, 0 ano, e da maior, 125 anos, e representa apenas o centro do intervalo observado. A própria idade máxima merece atenção, pois 125 anos é um valor biologicamente improvável, que pode indicar erro no preenchimento da data de nascimento, possibilidade que também se aplica a parte dos registros de crianças. Inconsistências desse tipo ilustram os problemas já apontados no uso estatístico dos boletins de ocorrência (Marcineiro *et al.*, 2022) e se somam à ausência de padronização dos registros criminais entre as unidades da Federação (Ipea, 2025). Ainda assim, as 97.120 vítimas com idade informada correspondem a 99,06% dos registros da base, cobertura suficiente para sustentar as medidas apresentadas.

4.3 ESTADO CIVIL

A Tabela 3 apresenta o quantitativo e o percentual de vítimas segundo o estado civil declarado no registro, informação que indica se a vítima possui ou possuía vínculo conjugal formalizado ou estável no momento do fato.

Tabela 3. Quantitativo e percentual de vítimas de crimes patrimoniais praticados por meio cibernético, por estado civil, no estado do Pará no período de 2022 a 2025.

Estado civil	Quantitativo	Percentual
Solteiro(a)	45.106	46,78%
Casado(a)	29.578	30,67%
União estável	13.335	13,83%
Divorciado(a)	5.275	5,47%
Viúvo(a)	3.137	3,25%
Total	**96.431**	**100,00%**

Em 1.062 casos não houve informação sobre o estado civil e, em 546, as vítimas eram pessoas jurídicas.
Fonte: Elaborado pelos autores a partir de dados do SIAC, setembro/2026.

As pessoas solteiras formam o maior grupo, com 45.106 registros (46,78%), seguidas pelas casadas, com 29.578 (30,67%), e pelas que vivem em união estável, com 13.335 (13,83%). Divorciados (5,47%) e viúvos (3,25%) respondem, juntos, por 8,72%. Agrupadas as categorias, 55,50% das vítimas declararam não ter vínculo conjugal no momento do registro, e 44,50% declararam viver em casamento ou união estável.

A predominância de solteiros deve ser lida com cautela, porque a própria literatura não oferece um padrão claro sobre a relação entre estado civil e vitimização por fraude. Nos Estados Unidos, a pesquisa nacional de vitimização incluiu, em 2017, um suplemento sobre fraudes respondido por cerca

de 51 mil pessoas com 18 anos ou mais, que informaram se, nos doze meses anteriores, haviam perdido dinheiro, sem recuperá-lo, em golpes de investimento, de compra de produtos e serviços, de falsos prêmios ou de relacionamento, entre outros, praticados por qualquer meio. Para cada estado civil, calculou-se a proporção de vítimas dentro do próprio grupo, isto é, o número de vítimas casadas dividido pelo total de pessoas casadas do país, e assim por diante, e o resultado foi de 1,00% entre as pessoas casadas, 1,35% entre as que nunca se casaram e 1,83% entre as divorciadas (Morgan, 2021). Em termos absolutos, a diferença entre essas taxas é pequena, inferior a um ponto percentual, ainda que a proporção entre divorciados seja quase o dobro da observada entre casados.

Há também indícios de que o peso do estado civil varie conforme o tipo de golpe. Em pesquisa com 1.375 consumidores dos Estados Unidos e do Canadá que relataram tentativas de golpe a uma plataforma de denúncias, as pessoas casadas tiveram menor probabilidade de perder dinheiro nos golpes baseados em oportunidade, categoria que reúne os golpes de romance, de investimento e de falsos prêmios, entre outros, e, nos demais tipos analisados, o estado civil não apareceu entre os fatores associados à perda (DeLiema *et al.*, 2022). Ainda assim, a associação não é consensual, pois revisão sistemática sobre golpes de romance registra estudo realizado na Malásia em que pessoas casadas apresentaram maior probabilidade de vitimização por esse golpe do que as que não estavam em um relacionamento (Bilz; Shepherd; Johnson, 2023).

4.4 PROFISSÃO

A Tabela 4 apresenta o quantitativo de vítimas segundo a profissão declarada no registro, limitado às vinte profissões mais frequentes da base.

Tabela 4. Quantitativo de vítimas de crimes patrimoniais praticados por meio cibernético, segundo as vinte profissões mais frequentes, no estado do Pará no período de 2022 a 2025.

Ranking	Profissão	Quantitativo
1	Aposentado(a)	5.836
2	Estudante	4.821
3	Dona de casa	4.796
4	Professor(a)	4.601
5	Vendedor(a)	3.199
6	Empresário(a)	2.916
7	Motorista	2.527
8	Doméstica	2.326
9	Comerciante	2.263
10	Auxiliar em geral	2.115
11	Lavrador(a)	1.941
12	Servidor(a) público(a)	1.902

Ranking	Profissão	Quantitativo
13	Administrador(a)	1.804
14	Agricultor(a)	1.772
15	Pescador(a)	1.609
16	Sem profissão	1.278
17	Técnico(a)	1.192
18	Engenheiro(a)	1.182
19	Advogado(a)	1.103
20	Operador(a)	987

16.665 registros foram lançados na categoria genérica “outras profissões”, o que sugere falhas no preenchimento do campo, e por isso não constam da tabela.
Fonte: Elaborado pelos autores a partir de dados do SIAC, setembro/2026.

Aposentados lideram a lista, com 5.836 registros, o equivalente a 5,95% do total da base, seguidos por estudantes (4.821; 4,92%), donas de casa (4.796; 4,89%) e professores (4.601; 4,69%). Essas quatro ocupações somam 20.054 registros, 39,97% das vinte primeiras posições. No conjunto, as vinte profissões mais frequentes reúnem 50.170 registros (51,17% da base), enquanto a categoria genérica “outras profissões” concentra 16.665 registros (17,00%), número quase três vezes maior que o da profissão mais citada. Os demais 31.204 registros distribuem-se entre profissões de menor frequência, registros sem informação e pessoas jurídicas.

Essas posições refletem também o tamanho de cada grupo na população, e não necessariamente um risco maior de vitimização, pois a proporção de vítimas dentro de cada profissão só poderia ser calculada com o total de pessoas em cada ocupação no estado, em categorias compatíveis com as do registro policial.

Quatro agrupamentos ajudam a interpretar a lista. O primeiro reúne pessoas sem ocupação remunerada declarada, como estudantes, donas de casa e pessoas sem profissão, que somam 10.895 registros (21,72% das vinte primeiras posições). Não ter ocupação remunerada, porém, não parece ser, por si só, um fator de risco, já que, no Japão, a situação de emprego, que distinguia trabalhadores em tempo integral de estudantes, donas de casa, desempregados e trabalhadores em tempo parcial, não esteve associada à vitimização por fraudes de consumo, incluídas as cibernéticas (Suzuki, 2024). Os aposentados, embora também estejam fora da atividade profissional, formam grupo à parte, pois recebem rendimento periódico na forma de benefício previdenciário, o que os aproxima, nesse aspecto, dos grupos com renda.

A liderança dos aposentados reforça a necessidade de atenção específica a esse público nas políticas de prevenção, dada a hipervulnerabilidade já descrita para pessoas idosas diante das fraudes bancárias eletrônicas (Volpato; Pegoraro Junior, 2024). Ainda assim, essa liderança não indica, por si só, que a aposentadoria eleve o risco, pois, na China, entre pessoas com 60 anos ou mais, as que

continuavam trabalhando tiveram maior chance de passar por situação de fraude do que as que não trabalhavam, sem diferença na chance de prejuízo financeiro (Hu; Andrade; Chen, 2026).

A segunda posição dos estudantes também pede cuidado, pois a categoria não informa a idade e pode abranger desde crianças e adolescentes até adultos que retomaram os estudos. Ainda assim, como crianças e adolescentes somam apenas 266 registros (Tabela 1), é provável que a maior parte dos estudantes vitimados tenha 18 anos ou mais, o que é compatível com a moda de 28 anos. Entre universitários chineses, as atividades on-line rotineiras aumentaram a chance de receber tentativas de fraude, mas a perda financeira esteve associada sobretudo a comportamentos on-line arriscados e ao baixo autocontrole (Lin *et al.*, 2025).

O segundo agrupamento reúne ocupações que, em regra, exigem formação de nível superior, como professores, engenheiros e advogados, com 6.886 registros, resultado coerente com o peso do ensino superior observado na Figura 2 e discutido na seção 4.5.

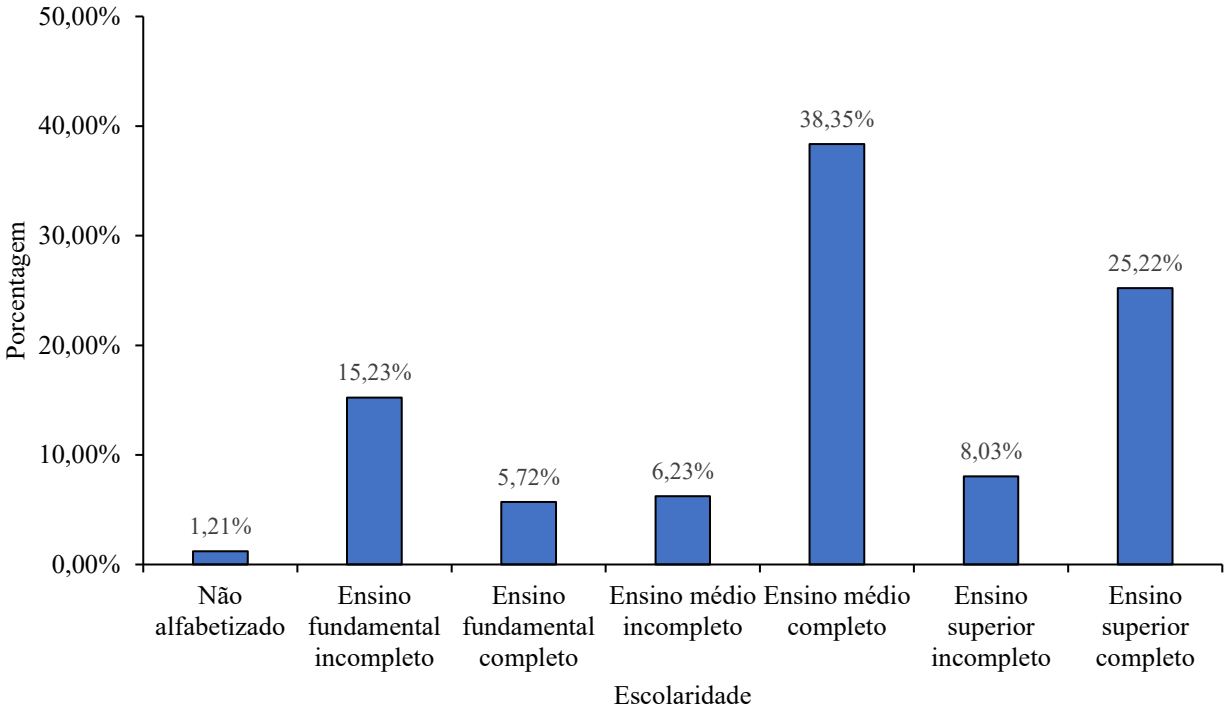
O terceiro agrupamento é formado por lavradores, agricultores e pescadores, com 5.322 registros (5,43% do total), o que sugere que a criminalidade patrimonial digital não se restringe aos centros urbanos e alcança trabalhadores do campo e da pesca. O quarto reúne vendedores, empresários e comerciantes, com 8.378 registros (8,55% do total), pessoas que fazem e recebem pagamentos com frequência no exercício da própria atividade. Uma hipótese é a de que parte desses casos envolva golpes praticados no contexto comercial, como pagamentos simulados ou negociações falsas.

A lista também reúne ocupações ligadas a serviços e ao trabalho manual, como motoristas (2.527), domésticas (2.326) e auxiliares em geral (2.115), que somam 6.968 registros (7,11% do total). O volume da categoria “outras profissões” revela uma limitação importante do registro. Quando cerca de um em cada seis boletins classifica a ocupação da vítima de forma genérica, perde-se informação valiosa para orientar a prevenção, problema que se soma às dificuldades já apontadas no uso de boletins de ocorrência como fonte estatística (Marcineiro *et al.*, 2022) e à ausência de padronização dos registros entre as polícias civis (Ipea, 2025).

4.5 ESCOLARIDADE

A Figura 2 apresenta, em gráfico de colunas, a distribuição percentual das vítimas segundo o nível de escolaridade informado no boletim de ocorrência, tomando como base os 95.633 registros com essa informação.

Gráfico 2. Percentual de vítimas de crimes patrimoniais praticados por meio cibernético, no estado do Pará no período de 2022 a 2025, por escolaridade.



Fonte: Elaborado pelos autores a partir de dados do SIAC, setembro/2026.

O ensino médio completo é o nível mais frequente, com 38,35% das vítimas (36.678 registros), seguido pelo ensino superior completo, com 25,22% (24.123). O ensino fundamental incompleto aparece em terceiro lugar, com 15,23% (14.569), e as demais categorias ficam abaixo de 9%, caso do ensino superior incompleto (8,03%), do ensino médio incompleto (6,23%), do ensino fundamental completo (5,72%) e dos não alfabetizados (1,21%). No conjunto, 71,61% das vítimas concluíram pelo menos o ensino médio, e 33,26% chegaram ao ensino superior, completo ou não, enquanto 22,16% não passaram do ensino fundamental completo.

Esses números não correspondem à imagem da vítima como pessoa de pouca instrução, e pesquisas de vitimização de outros países apontam na mesma direção. Na Austrália, a pesquisa nacional sobre fraude pessoal de 2021-2022 comparou a escolaridade das pessoas com a chance de cada grupo ter sido vítima de fraude, e constatou que, entre quem tinha alguma qualificação depois da escola, como certificado, diploma ou graduação, 9,5% sofreram fraude com cartão e 3,0% foram vítimas de golpes, enquanto, entre quem não tinha nenhuma qualificação desse tipo, os percentuais foram de 5,8% e 2,2%, respectivamente, o que indica que, naquele país, as pessoas com mais estudo apresentaram taxas de vitimização maiores do que as com menos estudo (ABS, 2023). Na Inglaterra e no País de Gales, mesmo levando em conta outros fatores, como idade, sexo e renda, quem não tinha

qualificação educacional apresentou menor chance de ser vítima de fraude do que quem tinha diploma de nível superior (ONS, 2026).

Em pesquisa nacional do DataSenado com 21.808 pessoas de 16 anos ou mais, quem perdeu dinheiro com crimes digitais nos doze meses anteriores tinha escolaridade um pouco mais alta que a do conjunto dos entrevistados, já que as pessoas com ensino superior, completo ou incompleto, eram 23% da amostra e 29% das vítimas, e as que tinham até o fundamental incompleto, 28% e 22%, respectivamente (DataSenado, 2024), enquanto na base do Pará essas faixas correspondem a 33,26% e 16,44% das vítimas registradas, o que sugere presença ainda maior dos mais escolarizados nos boletins de ocorrência, embora as duas fontes difiram quanto ao território, ao período e à forma de coleta.

Uma hipótese consistente com a forte presença de vítimas com ensino médio e superior é a da exposição. A pesquisa nacional de vitimização do Fórum Brasileiro de Segurança Pública e do Datafolha registrou, entre entrevistados da classe A/B, relatos mais frequentes de tentativas de golpe por falsas centrais de segurança (40,5% contra 23,4% nas classes C/D/E) e por Pix ou boleto (36,7% contra 21,9%), e uma das explicações apresentadas pelos autores para a maior vitimização desse estrato é o volume maior de interações digitais (FBSP; Datafolha, 2025). Se escolaridade, renda e intensidade de uso de serviços digitais caminharem juntas, a composição observada pode refletir um contato mais frequente com aplicativos bancários, compras pela internet e transferências instantâneas.

Uma segunda hipótese, que não exclui a primeira, é a de que pessoas mais escolarizadas registrem mais ocorrências, seja porque conhecem melhor os canais disponíveis, incluindo o registro eletrônico, seja porque recorrem com mais frequência ao boletim como apoio às tentativas de recuperar valores junto às instituições financeiras. Se for assim, a participação relativamente menor das pessoas de baixa escolaridade pode indicar subnotificação, e não menor vitimização, já que a vulnerabilidade do consumidor no ambiente digital, que inclui a falta de conhecimentos básicos para compreender a tecnologia utilizada (Lehfeld *et al.*, 2021), pode dificultar que essas pessoas percebam que foram vítimas ou saibam como registrar a ocorrência.

A categoria de ensino superior incompleto, com 7.684 registros (8,03%), é compatível com a presença de estudantes entre as profissões mais frequentes (Tabela 4), já que parte deles cursa a graduação. Essa convergência entre escolaridade e profissão sugere que os jovens universitários formam um subgrupo relevante para ações de prevenção desenvolvidas em parceria com as instituições de ensino.

Os 1.156 registros de vítimas não alfabetizadas, embora pouco numerosos, levantam a hipótese de que parte dessas pessoas dependa de terceiros para operar contas e aplicativos, situação que pode ampliar a exposição ao engano e dificultar a percepção de que houve fraude.

As hipóteses discutidas nesta seção têm implicações diferentes para a prevenção. A da exposição aponta para campanhas dirigidas a quem usa com frequência a internet e os aplicativos bancários, público que dificilmente se reconhece como vulnerável, enquanto a da possível subnotificação indica a necessidade de facilitar o registro e o acolhimento das vítimas de menor escolaridade.

5 CONCLUSÃO

Este estudo descreveu o perfil das vítimas de crimes patrimoniais praticados por meio cibernético registrados pela Polícia Civil do Pará de 2022 a 2025, a partir de 98.039 registros, e alcançou o objetivo proposto ao caracterizá-las quanto ao sexo, à idade, ao estado civil, à profissão e à escolaridade.

A vítima registrada é, sobretudo, uma pessoa adulta, com distribuição quase igual entre mulheres e homens, média ponderada de 41,84 anos e moda de 28 anos. Dois terços das vítimas têm de 20 a 49 anos, com maior participação na faixa de 30 a 39 anos, e as pessoas com 60 anos ou mais respondem por 15,80% dos registros, cerca de uma em cada seis vítimas. Predominam pessoas solteiras e, no conjunto, pessoas sem vínculo conjugal declarado, mas esse resultado deve ser lido com cautela, porque a base não permite saber se a condição conjugal se associa a maior ou menor risco de vitimização.

O achado mais expressivo diz respeito à escolaridade, pois 38,35% das vítimas têm ensino médio completo e 25,22%, ensino superior completo, e, somando-se os 8,03% com ensino superior incompleto, que já concluíram o ensino médio, chega-se a 71,61% das vítimas com pelo menos esse nível de instrução.

O resultado afasta a imagem da vítima como pessoa pouco instruída e é compatível com duas hipóteses complementares, a de que quem tem mais estudo usa com mais frequência a internet e os aplicativos bancários e, por isso, fica mais exposto aos golpes, e a de que essas pessoas têm maior propensão a registrar a ocorrência, o que pode sugerir uma maior subnotificação entre as vítimas de menor instrução.

Quanto à profissão, a presença de aposentados, estudantes, donas de casa e professores, ao lado de trabalhadores do campo, da pesca e do comércio, mostra que o fenômeno atravessa diferentes inserções sociais e reforça a necessidade de atenção especial aos grupos mais vulneráveis. A liderança

dos aposentados aponta para a proteção do público idoso, enquanto a presença de pessoas sem ocupação remunerada e de quem vive no campo e da pesca indica que a prevenção precisa chegar também a esses públicos, com linguagem acessível e por canais presentes no seu cotidiano.

Esses resultados oferecem subsídios concretos para a prevenção. Campanhas de conscientização tendem a ser mais eficazes quando segmentadas, alcançando tanto as pessoas que usam com frequência a internet e os aplicativos bancários, que raramente se veem como possíveis vítimas de golpes e fraudes, quanto os grupos mais vulneráveis apontados acima.

Para a Polícia Civil, recomenda-se aprimorar o preenchimento dos campos relativos à vítima, reduzindo o uso da categoria genérica “outras profissões” e validando a data de nascimento no momento do registro. Para as instituições financeiras e para a autoridade monetária, o perfil encontrado reforça a importância de mecanismos de proteção que não dependam apenas da atenção do usuário, como o rastreamento e o bloqueio de valores ao longo de toda a cadeia de contas envolvida na fraude e a interrupção de operações incompatíveis com o perfil do cliente, sobretudo diante de pessoas em situação de hipervulnerabilidade.

Como agenda de pesquisa, sugere-se relacionar essas distribuições à população residente, por meio de taxas por habitante, analisar o modo de execução descrito nos relatos dos registros e realizar pesquisas de vitimização no estado, capazes de estimar a parcela desses crimes que não chega ao conhecimento da polícia. Ao dar visibilidade a quem sofre o dano, este trabalho busca contribuir para que o enfrentamento desses crimes considere as pessoas que precisam ser protegidas.

REFERÊNCIAS

ABIN. Agência Brasileira de Inteligência. Engenharia social: guia para proteção de conhecimentos sensíveis. Brasília: ABIN, 2021. Disponível em: https://www.gov.br/abin/pt-br/institucional/acoes-e-programas/PNPC/boaspraticas/EngenhariaSocial_27062022.pdf. Acesso em: 17 out. 2026.

ABS. Australian Bureau of Statistics. Personal fraud, 2021-22 financial year. Canberra: ABS, 22 fev. 2023. Disponível em: https://www.abs.gov.au/statistics/people/crime-and-justice/personal-fraud/2021-22. Acesso em: 17 out. 2026.

ALMEIDA, F.; LOGSDON, L.; CECCATO, V.; PAULA, D. de; 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.

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.

BILZ, A.; SHEPHERD, L. A.; JOHNSON, G. I. Tainted love: a systematic literature review of online romance scam research. Interacting with Computers, Oxford, v. 35, n. 6, p. 773-788, 2023. DOI: 10.1093/iwc/iwad048. Disponível em: https://doi.org/10.1093/iwc/iwad048. Acesso em: 16 out. 2026.

BRASIL. Câmara dos Deputados. Projeto de Lei Nº 3.332, de 2025. Dispõe sobre a proteção de pessoas idosas contra fraudes financeiras em instituições financeiras e dá outras providências. Brasília, DF: Câmara dos Deputados, 2025. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2534298. Acesso em: 17 out. 2026.

BRASIL. Decreto-Lei Nº 2.848, de 7 de dezembro de 1940. Código Penal. Diário Oficial da União: seção 1, 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. Decreto-Lei Nº 3.689, de 3 de outubro de 1941. Código de Processo Penal. Diário Oficial da União: seção 1, Rio de Janeiro, 13 out. 1941. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm. Acesso em: 12 out. 2026.

BRASIL. Lei Nº 10.741, de 1º de outubro de 2003. Dispõe sobre o Estatuto da Pessoa Idosa e dá outras providências. Diário Oficial da União: seção 1, Brasília, DF, 3 out. 2003. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2003/l10.741.htm. Acesso em: 11 out. 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), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. Diário Oficial da União: seção 1, Brasília, DF, 28 maio 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm. Acesso em: 24 set. 2026.

BRASIL. Lei Nº 15.397, de 30 de abril de 2026. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), a fim de majorar as penas previstas para os crimes de furto, roubo, estelionato, receptação, receptação de animal e interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública, bem como para tipificar os crimes de receptação de animal doméstico e de fraude bancária. Diário Oficial da União: seção 1, Brasília, DF, 4 maio 2026. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/lei/L15397.htm. Acesso em: 17 out. 2026.

BURTON, A.; COOPER, C.; DAR, A.; MATHEWS, L.; TRIPATHI, K. Exploring how, why and in what contexts older adults are at risk of financial cybercrime victimisation: a realist review. Experimental Gerontology, v. 159, 111678, 2022. DOI: 10.1016/j.exger.2021.111678. Disponível em: https://doi.org/10.1016/j.exger.2021.111678. Acesso em: 17 out. 2026.

BUSSAB, W. O.; MORETTIN, P. A. Estatística básica. 10. ed. São Paulo: Saraiva, 2023.

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: 17 out. 2026.

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

CGI.br. Comitê Gestor da Internet no Brasil. Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros: TIC Domicílios 2024. São Paulo: CGI.br, 2025a. Disponível em: https://cetic.br/pt/tics/domicilios/2024/individuos/. Acesso em: 17 out. 2026.

CGI.br. Comitê Gestor da Internet no Brasil. TIC Kids Online Brasil 2025: principais resultados. São Paulo: CGI.br, 2025b. Disponível em: https://www.cetic.br/media/analises/tic_kids_online_brasil_2025_principais_resultados.pdf. Acesso em: 17 out. 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.

DATASENADO. Panorama político 2024: apostas esportivas, golpes digitais e endividamento. Brasília: Senado Federal, set. 2024. Disponível em: https://www12.senado.leg.br/noticias/arquivos/2024/09/30/relatorio_apostasesportivas-golpesdigitais-endividamento-1.pdf. Acesso em: 17 out. 2026.

DELIEMA, M.; LI, Y.; MOTTOLA, G. R. Correlates of responding to and becoming victimized by fraud: examining risk factors by scam type. International Journal of Consumer Studies, v. 47, n. 3, p. 1042-1059, 2023. DOI: 10.1111/ijcs.12886. Disponível em: https://doi.org/10.1111/ijcs.12886. Acesso em: 17 out. 2026.

DELIEMA, M.; LI, Y.; TAYLOR, M. K.; MOTTOLA, G. R. Does one size fit all?: an examination of risk factors by scam type. Washington, DC: FINRA Investor Education Foundation, 2022. (Insights: Financial Capability). Disponível em: https://www.finrafoundation.org/sites/finrafoundation/files/Does-One-Size-Fit-All-An-Examination-of-Risk-Factors-by-Scam-Type-Brief.pdf. Acesso em: 16 out. 2026.

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.

FBSP. Fórum Brasileiro de Segurança Pública; DATAFOLHA. Pesquisa de vitimização e percepção sobre violência e segurança pública 2025: um olhar sobre crime patrimonial e violência. São Paulo: FBSP, 2025. Disponível em: https://publicacoes.forumseguranca.org.br/server/api/core/bitstreams/33ed3320-fc11-45f9-a909-ed69eba48cfd/content. Acesso em: 11 out. 2026.

FRA. European Union Agency for Fundamental Rights. Online fraud: people's experiences across the EU. Vienna: FRA, 2026. Disponível em: https://fra.europa.eu/en/publication/2026/victims-online-fraud. Acesso em: 17 out. 2026.

FTC. Federal Trade Commission. Who experiences scams? A story for all ages. Washington, DC: FTC, 8 dez. 2022. (Data Spotlight). Disponível em: https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/12/who-experiences-scams-story-all-ages. Acesso em: 15 out. 2026.

GHAZI-TEHRANI, A. K.; PONTELL, H. N. Phishing evolves: analyzing the enduring cybercrime. Victims & Offenders, v. 16, n. 3, p. 316-342, 2021. DOI: 10.1080/15564886.2020.1829224. Disponível em: https://doi.org/10.1080/15564886.2020.1829224. Acesso em: 11 out. 2026.

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

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

GRECO, R. Curso de direito penal: parte especial. 22. ed. São Paulo: Atlas, 2025. v. 2.

HATFIELD, J. M. Social engineering in cybersecurity: the evolution of a concept. Computers & Security, v. 73, p. 102-113, mar. 2018. DOI: 10.1016/j.cose.2017.10.008. Disponível em: https://doi.org/10.1016/j.cose.2017.10.008. Acesso em: 17 out. 2026.

HAVERS, B.; TRIPATHI, K.; BURTON, A.; McMANUS, S.; COOPER, C. Cybercrime victimisation among older adults: a probability sample survey in England and Wales. PLoS ONE, San Francisco, v. 19, n. 12, e0314380, 2024. DOI: 10.1371/journal.pone.0314380. Disponível em: https://doi.org/10.1371/journal.pone.0314380. Acesso em: 17 out. 2026.

HU, T.; ANDRADE, F. C. D.; CHEN, Y.-C. Multilevel risk factors for financial fraud in later life: evidence from China. Innovation in Aging, Oxford, v. 10, n. 4, igag004, 2026. DOI: 10.1093/geroni/igag004. Disponível em: https://doi.org/10.1093/geroni/igag004. Acesso em: 16 out. 2026.

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

IBGE. Instituto Brasileiro de Geografia e Estatística. Censo Demográfico 2022: tabela 9514: população residente, por sexo, idade e forma de declaração da idade. Rio de Janeiro: IBGE, 2023b. Disponível em: https://sidra.ibge.gov.br/tabela/9514. Acesso em: 13 out. 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.

JAVELIN STRATEGY & RESEARCH. Child identity fraud: a web of deception and loss. Livonia, MI: Javelin Strategy & Research, 2021. Disponível em: https://javelinstrategy.com/sites/default/files/files/reports/21-5012J-FM-2021%20Child%20Identity%20Fraud%20Study_1.pdf. Acesso em: 15 out. 2026.

KÖBIS, N. C.; DOLEŽALOVÁ, B.; SORAPERRA, I. Fooled twice: people cannot detect deepfakes but think they can. iScience, v. 24, n. 11, 103364, 2021. DOI: 10.1016/j.isci.2021.103364. Disponível em: https://doi.org/10.1016/j.isci.2021.103364. Acesso em: 17 out. 2026.

KONING, L.; JUNGER, M.; VELDKAMP, B. Risk factors for fraud victimization: the role of socio-demographics, personality, mental, general, and cognitive health, activities, and fraud knowledge. International Review of Victimology, v. 30, n. 3, p. 443-479, 2024. DOI: 10.1177/02697580231215839. Disponível em: https://doi.org/10.1177/02697580231215839. Acesso em: 17 out. 2026.

KRISTIANSEN, S. G.; JENSEN, A. V. Victimization in online gaming-related trade scams: a study among young Danes. Nordic Journal of Criminology, Oslo, v. 24, n. 2, p. 1-17, 2023. DOI: 10.18261/njc.24.2.6. Disponível em: https://doi.org/10.18261/njc.24.2.6. Acesso em: 17 out. 2026.

LAI, S.; MOURÃO, P. B. Lei nº 14.155/2021 dos crimes cibernéticos. Revista do Ministério Público do Estado do Rio de Janeiro, Rio de Janeiro, n. 82, p. 233-241, out./dez. 2021. Disponível em: https://www.mprj.mp.br/servicos/revista-do-mp/revista-82/artigo-das-pags-233-241. Acesso em: 11 out. 2026.

LAY, W.; ARIEL, B.; HARINAM, V. Recalibrating the police to focus on victims using police records. Policing: A Journal of Policy and Practice, v. 17, paac053, 2023. DOI: 10.1093/police/paac053. Disponível em: https://doi.org/10.1093/police/paac053. Acesso em: 11 out. 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.

LEHFELD, L. S.; CELIOT, A.; SIQUEIRA, O. N.; BARUFI, R. B. A (hiper)vulnerabilidade do consumidor no ciberespaço e as perspectivas da LGPD. Revista Eletrônica Pesquiseduca, Santos, v. 13, n. 29, p. 236-255, 2021. DOI: 10.58422/repesq.2021.e1029. Disponível em: https://periodicos.unisantos.br/pesquiseduca/article/view/1029. Acesso em: 11 out. 2026.

LIMA, R. B. Manual de processo penal: volume único. 15. ed. Salvador: JusPodivm, 2026.

LIN, K.; WU, Y.; SUN, I. Y.; QU, J. Telecommunication and cyber fraud victimization among Chinese college students: an application of routine activity theory. Criminology & Criminal Justice, v. 25, n. 3, p. 717-735, 2025. DOI: 10.1177/17488958221146144. Disponível em: https://doi.org/10.1177/17488958221146144. Acesso em: 16 out. 2026.

LOPES JR., Aury. Direito processual penal. 23. ed. São Paulo: SaraivaJur, 2026.

MAHER, C. A.; McNEALEY, R. L.; FISHER, T.; KRUPA, J. M.; HOLT, T. J. Assessing the gendered risks of online fraud victimization in a general population sample. Crime & Delinquency, 2026. DOI: 10.1177/00111287261453812. Disponível em: https://doi.org/10.1177/00111287261453812. Acesso em: 17 out. 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.

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

MORGAN, R. E. Financial fraud in the United States, 2017. Washington, DC: Bureau of Justice Statistics, 2021. (NCJ 255817). Disponível em:https://bjs.ojp.gov/library/publications/financial-fraud-united-states-2017. Acesso em: 16 out. 2026.

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.

NUCCI, G. S. Manual de direito penal: volume único. 21. ed. Rio de Janeiro: Forense, 2025.

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.

ONS. Office for National Statistics. Fraud and computer misuse in England and Wales: year ending March 2025. Newport: ONS, 2026. Disponível em: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/natureoffraudandcomputermisuseinenglandandwales/yearendingmarch2025. Acesso em: 16 out. 2026.

PARTI, K. What is a capable guardian to older fraud victims? Comparison of younger and older victims' characteristics of online fraud utilizing routine activity theory. Frontiers in Psychology, Lausanne, v. 14, 1118741, 2023. DOI: 10.3389/fpsyg.2023.1118741. Disponível em: https://doi.org/10.3389/fpsyg.2023.1118741. Acesso em: 17 out. 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.

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.

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.

SIQUEIRA, E. Combate digital: prevenção e repressão de fraudes bancárias e golpes digitais: como enfrentar a nova realidade dos crimes cibernéticos que afetam sociedade, negócios e segurança pública. Brasília: Ix Editora, 2024.

SOUSA, A. S.; OLIVEIRA, G. S.; ALVES, L. H. A pesquisa bibliográfica: princípios e fundamentos. Cadernos da FUCAMP, Uberlândia, v. 20, n. 43, p. 64-83, 2021. Disponível em: https://revistas.fucamp.edu.br/index.php/cadernos/article/view/2336. Acesso em: 12 out. 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, e3604, 2025. DOI: 10.54899/dcs.v22i84.3604. Disponível em: https://doi.org/10.54899/dcs.v22i84.3604. Acesso em: 24 set. 2026.

SOUZA, F. M. Sextorsão e romance scam no estado do Pará. 2022. 88 f. Dissertação (Mestrado em Segurança Pública) - Programa de Pós-Graduação em Segurança Pública, Universidade Federal do Pará, Belém, 2022. Disponível em: https://www.ppgsp.propesp.ufpa.br/ARQUIVOS/teses_e_dissertacoes/dissertacoes/2020/202005%20-%20FERNANDA%20MAUES%20DE%20SOUZA.pdf. Acesso em: 11 out. 2026.

SUZUKI, A. Routine activities and consumer fraud victimization: findings from a social survey in Chiba Prefecture, Japan. Crime Prevention and Community Safety, v. 26, n. 4, p. 373-384, 2024. DOI: 10.1057/s41300-024-00219-2. Disponível em: https://doi.org/10.1057/s41300-024-00219-2. Acesso em: 16 out. 2026.

VOCE, I.; MORGAN, A. Cybercrime in Australia 2023. Canberra: Australian Institute of Criminology, 2023. (Statistical Report, 43). DOI: 10.52922/sr77031. Disponível em: https://www.aic.gov.au/sites/default/files/2023-06/sr43_cybercrime_in_australia_2023.pdf. Acesso em: 17 out. 2026.

VOLPATO, M. S.; PEGORARO JUNIOR, P. R. Hipervulnerabilidade do idoso em fraudes bancárias eletrônicas. In: ENCONTRO VIRTUAL DO CONPEDI, 7., 2024, Florianópolis. Direito, globalização e responsabilidade nas relações de consumo. Florianópolis: CONPEDI, 2024. p. 196-214. Disponível em: https://site.conpedi.org.br/publicacoes/v38r977z/033oy6hg/ULWK7vwz0fq5vtQi.pdf. Acesso em: 17 out. 2026.

WENDT, E. Investigação criminal cibernética no Brasil. São Paulo: Mizuno, 2024.