6 - Fraude Eletrônica na Região Metropolitana de Belém: Perfil de Vitimização e Padrões Temporais (2021-2024)

Electronic Fraud in the Belém Metropolitan Area: Victimization Profile and Temporal Patterns (2021-2024)

Thiago Galvao Sobrinho[1]
Edson Marcos Leal Soares Ramos[2]

RESUMO

A Era Digital redefiniu as relações sociais, mas também criou um ambiente fértil para crimes informáticos impróprios, como a fraude eletrônica, uma forma de crime patrimonial. Com a popularização do PIX e dispositivos móveis, a criminalidade migrou para o ambiente virtual na busca pelo lucro e anonimato. O artigo objetiva analisar o perfil de vitimização e a incidência da fraude eletrônica na Região Metropolitana de Belém. Busca-se caracterizar o comportamento temporal do crime e o perfil sociodemográfico das vítimas, abrangendo variáveis de gênero, idade e instrução. Trata-se de uma pesquisa quantitativa e descritiva baseada em 21.813 boletins de ocorrência policial, utilizando-se de estatística descritiva para organizar os dados primários. Os resultados revelaram um crescimento de 480% nas ocorrências no período de 2021 a 2024. A análise temporal mostra que 85% dos crimes ocorrem em dias úteis e 80% em turnos diurnos, coincidindo com o horário comercial e os limites bancários vigentes. O perfil das vítimas é predominantemente feminino (54%), solteiro (53,32%) e com alta escolaridade (86% possuem ao menos ensino médio completo), indicando que a vitimização não se restringe a grupos de menor escolaridade. Os dados indicam que o delito envolve o uso de engenharia social para explorar gatilhos emocionais das vítimas. O estudo ressalta a urgência de capacitação investigativa especializada e campanhas de letramento digital para autoproteção da sociedade.

Palavras-chave: PIX; Engenharia social; Crimes Patrimoniais.

1 Investigador da Polícia Civil do Estado do Pará. Mestre em Segurança Pública (UFPA). Graduado em Direito (Universidade da Amazônia). Especialista em Gestão Pública com ênfase em Gestão do Conhecimento nas Organizações Pública (EGPA) e Pós-graduado em Inteligência de Segurança Pública (Academia Nacional de Polícia). E-mail: thiago.galvao.sobrinho@gmail.com.

2 Doutor em Engenharia de Produção. Mestre em Estatística (UFPE). Bacharel em Estatística (UFPA). E-mail: ramosedson@gmail.com.

ABSTRACT

The Digital Age has redefined social relations, but it has also created a fertile environment for improper computer crimes, such as electronic fraud a form of property crime. With the popularization of PIX and mobile devices, criminality has migrated to the virtual environment in search of profit and anonymity. This article aims to analyze the victimization profile and the incidence of electronic fraud in the Belém Metropolitan Area. It seeks to characterize the temporal behavior of the crime and the sociodemographic profile of the victims, covering variables of gender, age, and education. This is a quantitative and descriptive study based on 21,813 police reports, utilizing descriptive statistics to organize the primary data. The results revealed a 480% growth in occurrences between 2021 and 2024. Temporal analysis shows that 85% of crimes occur on weekdays and 80% during daytime shifts, coinciding with business hours and prevailing banking limits. The victim profile is predominantly female (54%), single (53.32%), and highly educated (86% have at least a high school diploma), indicating that victimization is not restricted to groups with lower education levels. The data indicate that the offense involves the use of social engineering to exploit victims' emotional triggers. The study highlights the urgent need for specialized investigative training and digital literacy campaigns for societal self-protection.

Keywords: PIX; Social engineering; Property crimes.

1 INTRODUÇÃO

A humanidade está em constante modificação, passando por uma atual revolução informacional, na qual o processamento de dados e a velocidade de comunicação que ocorrem em escala global tornaram-se um dos pilares do mundo de hoje (Roza, 2017). Este fenômeno, denominado Era Digital, caracteriza-se pelo uso da tecnologia da informação e comunicação em todas as áreas da atividade humana, redefinindo os relacionamentos sociais (Sydow, 2022). A internet, nesse contexto, deixa de ser apenas um serviço para se tornar um verdadeiro ecossistema virtual complexo, superando as barreiras geográficas e temporais (Santoro*et al.*, 2020), ainda mais com a popularização dos dispositivos móveis que facilitou o acesso à informação e aos serviços online (Nery; Britto, 2022).

Nesse ciberespaço, mesmo diante de todos os avanços e benefícios sociais relacionados ao avanço tecnológico, configura-se um campo fértil para condutas ilícitas inovadoras e complexas (Silveira, 2015). A criminalidade adaptou-se ao desenvolvimento tecnológico, fazendo uso desta ferramenta para obter o maior lucro possível e um alcance bem mais abrangente de vítimas sob a falsa sensação de anonimato e impunidade (Arsawati; Darma; Antari, 2021; Silva, 2020).

Esses delitos que ocorrem no ambiente virtual são classificados pela doutrina como crimes informáticos próprios, voltados contra os próprios sistemas informáticos e dados, e impróprios, que apenas se valem da tecnologia como meio para a realização do crime, em que a infração de rua migra para o ambiente virtual, como é o caso dos crimes de estelionato cometidos pelo meio digital (Almeida, 2023; Crespo, 2011). Os criminosos realizam esta migração do mundo real para o digital vislumbrando um menor risco de identificação e penas mais brandas para essa forma de delito (Silva, 2020). Assim, o crime cibernético apresenta-se como um fenômeno complexo que exige esforço conjunto de aperfeiçoamento das forças de segurança pública na busca de um enfrentamento eficaz (Justiniano, 2017).

Dentre as infrações penais de grande incidência no ambiente virtual, destaca-se a fraude eletrônica, que é uma modalidade qualificada do estelionato, previsto no art. 171, § 2º-A, do Código Penal Brasileiro (Brasil, 1940), introduzido pela Lei nº 14.155 (Brasil, 2021), tratando-se de um crime informático impróprio, em que a internet é apenas o meio para o cometimento do crime. Este delito consiste em induzir a vítima a erro, por meio de informações fornecidas em redes sociais, e-mails, ligações telefônicas e plataformas de vendas online, para a obtenção da vantagem ilícita (Alcadipani; Lima; Bueno, 2024).

O prejuízo causado por essas ações criminosas atinge grandes valores monetários e fere princípios primordiais como a dignidade da pessoa humana e a segurança das relações financeiras (Lima, 2020; IBM Security, 2023). Neste contexto, a tecnologia serve como um escudo para a atuação do criminoso que passa a ter um alcance maior de possíveis vítimas, sem a necessidade de presença física, diminuindo os riscos de ser flagrado cometendo o ilícito. Existem estudos que demonstram que o Cartel no México possui centrais telefônicas para cometer golpes contra aposentados nos Estados Unidos, enquanto no Brasil, investigações já apontam que tanto o Primeiro Comando da Capital (PCC) quanto o Comando Vermelho (CV) possuem centrais para o cometimento da fraude eletrônica, fazendo uso tanto do Pix quanto de contas de terceiros (Alcadipani*et al.*, 2024).

Dessa forma, considerando o cenário da expansão dos delitos virtuais, o presente artigo tem por objetivo analisar o perfil da vitimização e atuação da fraude eletrônica na Região Metropolitana de Belém (RMB), baseando-se em dados consolidados pelo Sistema Integrado de Segurança Pública nos anos de 2021 a 2024. Por meio de uma abordagem quantitativa e

descritiva, busca-se caracterizar o comportamento temporal do fenômeno e o perfil sociodemográfico das vítimas, incluindo variáveis como gênero, faixa etária, grau de instrução, dentre outros.

O estudo se desenvolveu por meio de uma abordagem quantitativa e de natureza descritiva, voltada ao mapeamento e à análise estatística de dados oriundos do Sistema Integrado de Segurança Pública (SISP), a partir de ocorrências registradas de fraude eletrônica. Tendo como lócus a Região Metropolitana de Belém (RMB) no período de 2021 a 2024, as técnicas estatísticas descritivas permitiram a organização sistemática e padronizada dos registros de estelionato digital no referido espaço geográfico e temporal (Gil, 2008).

A RMB foi a delimitação geoespacial do presente estudo, visto que a macrorregião é formada pelos municípios de Belém, Ananindeua, Marituba, Benevides, Santa Bárbara do Pará, Santa Izabel do Pará, Castanhal e Barcarena, sendo que, mais à frente do estudo, será possível observar que nem todos possuem ocorrências sobre fraude eletrônica no recorte temporal da pesquisa. A RMB concentra uma população de 2.370.174 habitantes, bem como boa parte da economia paraense, sendo que Belém tem uma economia formada por 86% de serviços no PIB (IBGE, 2023).

Os dados primários desta pesquisa foram fornecidos pela Secretaria de Inteligência e Análise Criminal (SIAC) e foram organizados em planilha eletrônica, tendo como características ocorrências no período de 2021, ano em que a fraude eletrônica foi tipificada no Código Penal por meio da Lei nº 14.155/2021 (Brasil, 2021), a 2024, tipificadas como estelionato, em que o local do crime foi redes sociais/internet, com a ocorrência do fato na RMB. A base de dados resultou em 21.813 boletins de ocorrência policial (BOPs).

Foram consideradas as seguintes variáveis: (i) ano e mês; (ii) dia da semana; (iii) turno; (iv) profissão; (v) grau de instrução da vítima; (vi) estado civil da vítima; (vii) faixa etária; (viii) sexo; (ix) município. A análise dos dados foi realizada por meio de estatística descritiva, a partir de frequências absolutas e relativas para cada variável, visando descrever uma visão geral e fiel do fenômeno (Bussab; Morettin, 2017).

Cabe ressaltar que o presente estudo se limita à estatística descritiva, com o objetivo de mapear frequências e padrões nos dados disponíveis, não empregando técnicas de estatística inferencial (como testes de hipótese, correlação ou regressão). Dessa forma, as relações apresentadas ao longo

da análise devem ser compreendidas como associações observacionais, não sendo possível estabelecer relações de causalidade entre as variáveis sociodemográficas, temporais e a ocorrência do delito.

Ressalta-se, ainda, que os resultados obtidos refletem as particularidades socioeconômicas e criminais da Região Metropolitana de Belém, não devendo ser generalizados de forma automática para outras regiões do país, que podem apresentar dinâmicas distintas de digitalização financeira, perfil populacional e atuação das forças de segurança.

É importante destacar, também, que a base de dados fornecida pela Secretaria de Inteligência e Análise Criminal (SIAC) não contempla variáveis relativas à renda ou à raça/cor das vítimas, o que constitui uma limitação relevante para a análise de vitimização em crimes patrimoniais. A ausência desses marcadores sociais impede a verificação de possíveis efeitos de composição populacional, desigualdade de acesso a serviços financeiros digitais e outros fatores estruturais que podem influenciar tanto a exposição ao risco quanto o próprio registro da ocorrência policial.

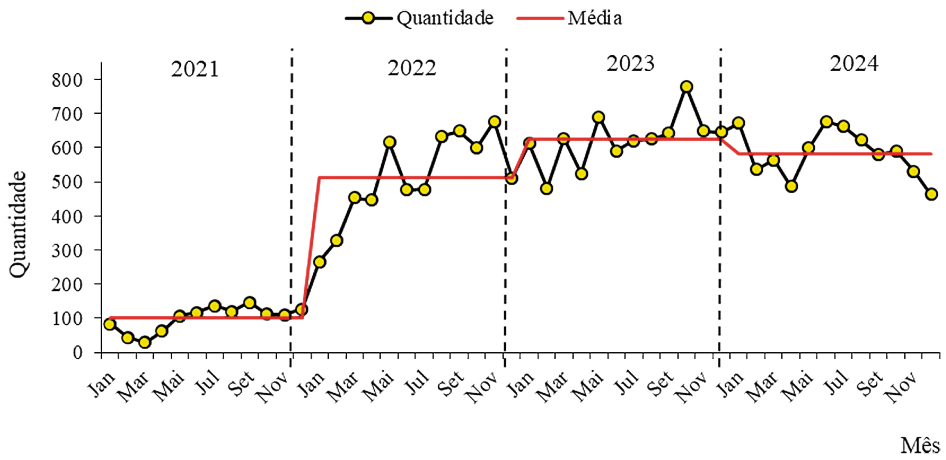
As análises de frequência por dia da semana e turno do dia baseiam-se exclusivamente no número absoluto de ocorrências registradas, sem acesso a dados sobre o volume total de transações financeiras (bancárias e via Pix) realizadas nesses mesmos períodos. Isso significa que os resultados refletem a quantidade de registros policiais, e não necessariamente uma taxa de incidência proporcional ao volume de operações financeiras, o que deve ser considerado na interpretação dos achados.

Adicionalmente, os dados utilizados referem-se exclusivamente a boletins de ocorrência registrados, estando sujeitos à subnotificação característica de crimes patrimoniais, especialmente entre vítimas que optam por não formalizar a denúncia.

2 DESENVOLVIMENTO

O estudo dos 21.813 BOPs relacionados ao crime de fraude eletrônica ocorridos na RMB tornou possível uma compreensão mais apurada sobre o fenômeno para futuros estudos acadêmicos, políticas públicas e ações das forças de segurança pública do estado do Pará. A evolução do número de ocorrências registradas no período de 2021 a 2024 (Figura 1) evidencia um forte crescimento e posterior estabilização em patamar elevado do fenômeno.

Figura 1 - Quantidade de registros de Fraude Eletrônica, ocorridos na Região Metropolitana de Belém, no período de 2021 a 2024, por ano e mês



Fonte: Construção do autor a partir de dados do SIAC (2025).

Lima (2020) afirma que o Brasil passa por uma consolidação de uma nova dinâmica nos crimes patrimoniais, tendo por característica a migração das atividades ilícitas para o ambiente digital, fenômeno este que está associado diretamente ao crescimento considerável das transações bancárias eletrônicas e serviços digitais. O período analisado demonstrou um crescimento exponencial no volume de ocorrências do ano de 2021 (1.202 ocorrências) ao ano de 2024 (6.985 ocorrências), achado que se aproxima da dinâmica de reorganização das estruturas criminais descrita por Feltran (2018) frente às inovações tecnológicas.

O crescimento acentuado identificado no ano de 2021 para o ano de 2022 também é apontado por Nascimento (2024) em relação a ocorrências relacionadas a crimes cibernéticos, em que o autor aponta um aumento de 87%, sendo a criação do Pix apontada como um fator de impacto nesses números. Monteiro e Ramos (2021) apontam que a pandemia da Covid-19

também teve grande impacto no elevado registro destas modalidades criminosas, visto o uso da internet para comunicação, aplicativos financeiros e compras online em geral, tudo em razão do isolamento social ocorrido no período.

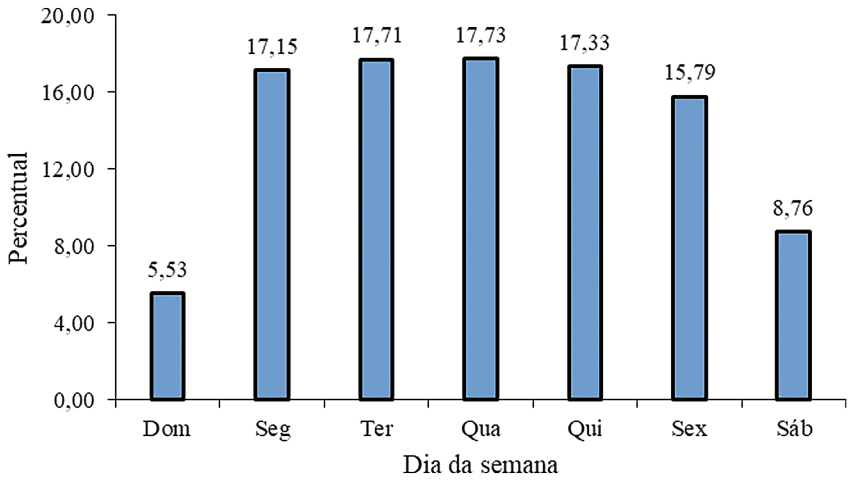
Alves (2023) acrescenta que esse aumento de crimes digitais, advindo da sofisticação das organizações criminosas nesta prática delituosa, torna o enfrentamento investigativo um grande desafio que exige uma ação conjunta e coordenada entre o direito penal, o uso de tecnologia e as políticas de segurança pública, em virtude da complexidade do delito. Este cenário foi agravado devido ao período da pandemia de Covid-19, visto que o isolamento social gerou uma migração em massa das transações e interações sociais para o ambiente virtual, ampliando o alcance dos infratores (Costa; Abrantes, 2023; Oliveira*et al.*, 2024).

Nos anos de 2022 (6.138 ocorrências), 2023 (7.488 ocorrências) e 2024 (6.985 ocorrências), foi possível detectar uma tendência de manutenção nos registros de ocorrências relacionadas ao delito de fraude eletrônica, na qual houve um aumento seguido de pequena queda neste período, necessitando de acompanhamento nos anos seguintes para verificar se o fenômeno está em processo de estabilização. Paralelamente, identificam-se oportunidades de atuação na área da segurança pública que possam contribuir para a redução dos casos.

Com relação aos meses, destaca-se outubro de 2023 como o pico de ocorrências do crime de fraude eletrônica, com um total de 779 casos, bem como janeiro de 2021 como o menor número de ocorrências, ressaltando que neste ano houve a tipificação legal do crime (Brasil, 2021), quando os estados ainda se adaptavam ao registro desta nova modalidade criminosa, o que pode ter contribuído para os baixos números do ano.

A distribuição percentual dos crimes de fraude eletrônica na Região Metropolitana de Belém (2021 a 2024), segmentados pelo dia da semana (Figura 2), visa compreender o comportamento do fenômeno criminal, correlacionando com atividades cotidianas e sua possível influência no delito.

Figura 2 - Percentual de registros de Fraude Eletrônica, ocorridos na Região Metropolitana de Belém, no período de 2021 a 2024, por dia da semana



Fonte: Construção do autor a partir de dados do SIAC (2025).

Diante deste cenário semanal, é possível perceber uma concentração de ocorrências de segunda a sexta-feira (oscilando de 15,79% a 17,73%), com grande queda no sábado (8,76%) e domingo (5,53%), ressaltando que grande parte desta forma de delito ocorre em dias chamados úteis, ou seja, com o funcionamento de estabelecimentos comerciais e serviços bancários.

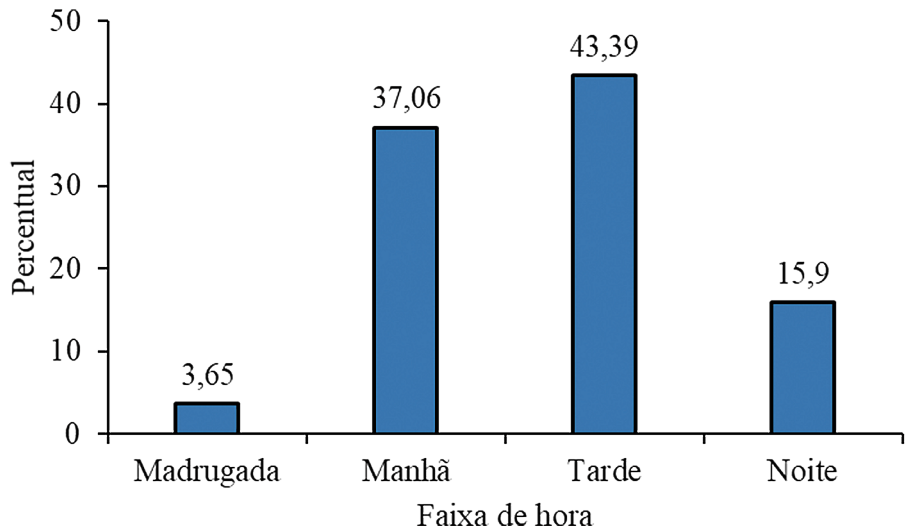
De segunda a sexta-feira são concentrados aproximadamente 85% do total de ocorrências registradas durante a semana, coincidindo com os dias de maior movimentação financeira e interações de serviços bancários, contrastando com o final de semana, que representa menos de 15% dos casos, o que leva a corroborar a ideia de Misse (1997), que afirma que as estruturas criminais se organizam em resposta às oportunidades estruturais do sistema econômico formal, no qual, quando se refere ao crime de fraude eletrônica, este se coaduna aos dias de maior movimentação financeira e interações de serviços bancários.

O próprio Banco Central do Brasil (BACEN, 2025) apresenta dados de consolidação do Pix como o principal meio de transferência de valores entre os brasileiros e aponta que, no período de 2020 a 2022,

a quantidade de Pix realizados de segunda a sexta-feira concentrou a maior parte das transações e dos valores movimentados, chegando a aproximadamente 77% do total, com queda considerável no final de semana. Esse padrão acompanha as dinâmicas das relações sociais e financeiras contemporâneas.

Na sequência da análise, agora se estendendo ao turno do fato (Figura 3), é possível identificar que há uma maior concentração nos turnos da manhã e da tarde na ocorrência do delito, que representam aproximadamente 80% dos casos em estudo.

Figura 3 - Percentual de registros de Fraude Eletrônica, ocorridos na Região Metropolitana de Belém, no período de 2021 a 2024, por Turno do Dia



Fonte: Construção do autor a partir de dados do SIAC (2025).

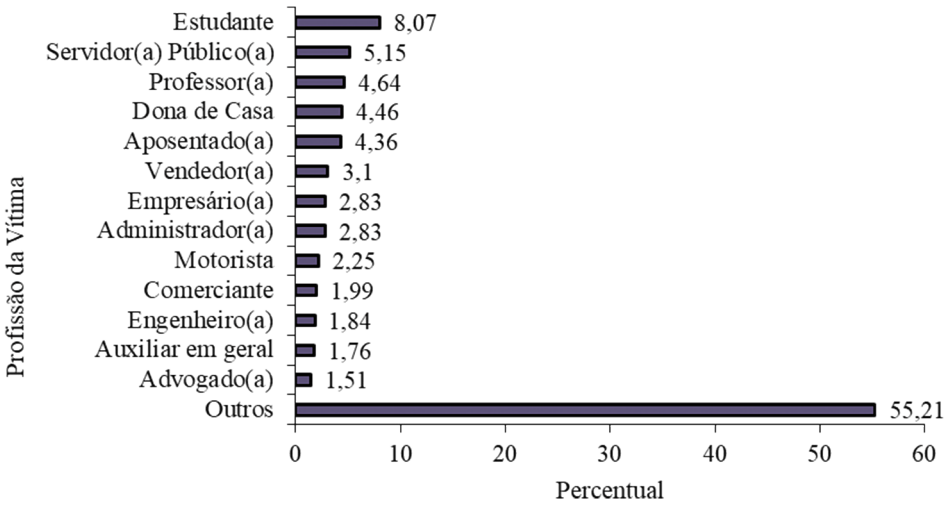
A distribuição por turno acompanha os padrões de rotina da atividade comercial (Nascimento, 2024). Outros pesquisadores já demonstravam esse padrão na incidência de crimes tecnológicos em horários de maior uso de transações bancárias e o uso de redes sociais (Silva; Azevedo, 2022). O próprio site do Banco Central do Brasil (2025) apresenta informações de que há limites estabelecidos para transações financeiras que ocorram

no período da noite, o que impulsiona a maior atividade criminosa nos demais turnos.

O turno da madrugada, com apenas 3,65%, apresenta a menor concentração de ocorrências, coincidindo com o período de maiores restrições bancárias e menor movimentação financeira. Esta análise estatística descritiva é fundamental para o planejamento de políticas públicas de atuação policial no enfrentamento desta modalidade criminosa, compreendendo como o fenômeno se comporta.

A análise do fenômeno das fraudes eletrônicas exige um foco detalhado nas características das vítimas, especialmente quanto à profissão declarada. Para viabilizar o estudo, diante da variedade de dados, foram destacadas 11 profissões com maior incidência, agrupando-se as demais na categoria outros (Figura 4).

Figura 4 - Percentual de registros de Fraude Eletrônica, ocorridos na Região Metropolitana de Belém, no período de 2021 a 2024, por Profissão da Vítima (11 maiores ocorrências)



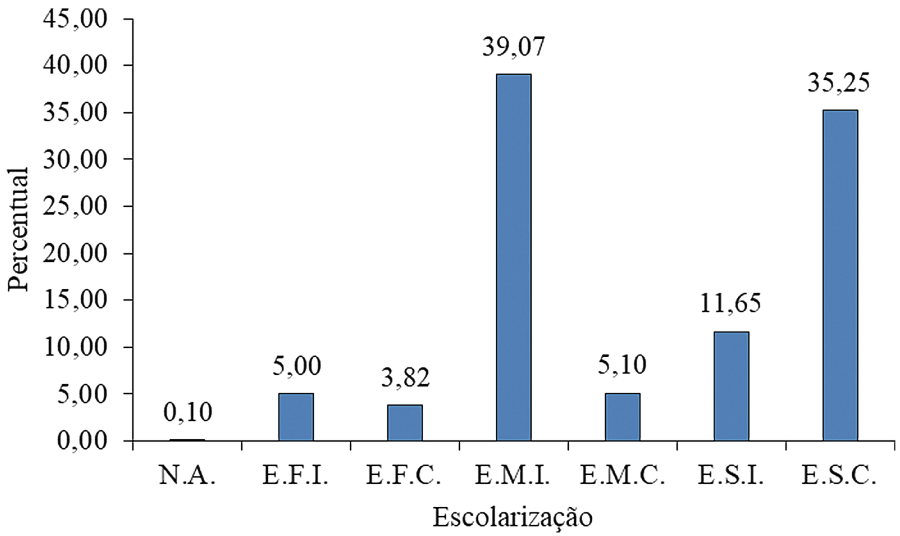
Fonte: Construção do autor a partir de dados do SIAC (2025).

A análise (Figura 4) possibilita uma interpretação da democratização do ciberdelito, no caso, a fraude eletrônica, visto esta alcançar vítimas de diversos grupos profissionais, apresentando o alcance do criminoso. A categoria 'Outros', com 55,21% das profissões das vítimas, é um indicador de que este delito não se concentra em apenas algumas ocupações, revelando um padrão de vulnerabilidade generalizado.

Segundo Domingos e Jacob (2024), o criminoso cibernético tem por perfil explorar vulnerabilidades comuns em interações *online*, independentemente da ocupação exercida pela vítima, tendo por prioridade alvos com rotinas conectadas. Observa-se que estudantes (8,07%) e servidores públicos (5,15%) figuram entre as maiores ocorrências, e a doutrina aponta que existe uma lacuna grave na formação digital dos cidadãos, o que permite que o crime atinja diferentes níveis sociais, sem fronteiras claramente distinguidas (Lopes; Lopes, 2023).

É possível identificar a multiplicidade e diversidade de profissões atingidas, desde donas de casa (4,46%), administradores (2,83%) e engenheiros (1,84%) até aposentados (4,36%), o que indica a diversidade de perfis profissionais entre as vítimas (Zacarias; Freire, 2023). Quanto à escolarização das vítimas (Figura 5), foi possível compreender que o Ensino Médio Completo (EMC) lidera com 39,12%, seguido do Ensino Superior Completo (ESC) com 35,29% e Ensino Superior Incompleto (ESI) com 11,66% das vítimas. Os menores índices ficaram com Ensino Médio Incompleto (EMI) 5,10%, Ensino Fundamental Incompleto (EFI) 5,01%, e Ensino Fundamental Completo (EFC) com 3,82% das vítimas.

Figura 5 - Percentual de registros de Fraude Eletrônica, ocorridos na Região Metropolitana de Belém, no período de 2021 a 2024, por Escolarização da Vítima



Fonte: Construção do autor a partir de dados do SIAC (2025).

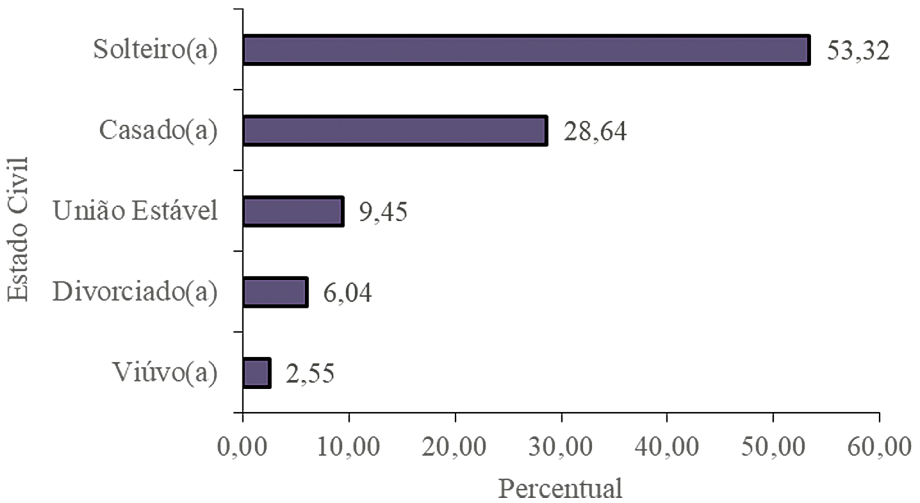
Nota: N.A. – Não Alfabetizado(a); E.F.I. – Ensino Fundamental Incompleto; E.F.C. – Ensino Fundamental Completo; E.M.I. – Ensino Médio Incompleto; E.M.C. – Ensino Médio Completo; E.S.I. – Ensino Superior Incompleto; E.S.C. – Ensino Superior Completo.

Estes dados indicam que a vitimização por fraude eletrônica atinge também pessoas com maior escolaridade, contrariando a ideia de que apenas indivíduos com menor instrução seriam alvos preferenciais, pois a soma daqueles que iniciaram o ensino superior e daqueles que já têm o ensino superior ultrapassa a marca de 46%, indicando que o acesso à informação pode não ser suficiente para garantir segurança cibernética nos dias de hoje.

Os dados de ensino superior completo, com mais de 35% das vítimas, indicam que os criminosos se utilizam de toda a forma de engenharia social necessária para induzir a erro todo o tipo de vítimas, das menos instruídas às com maior grau de instrução acadêmica. Souza (2022) discute que as táticas relacionadas à fraude digital denominada *Romance Scam* independem do grau intelectual da vítima, focando em gatilhos emocionais e na confiança da vítima nas relações virtuais.

Quando se trata do estado civil das vítimas (Figura 6), as que se declararam solteiras são maioria absoluta, com 53,32% no período de 2021 a 2024, seguidas de indivíduos que se manifestaram como casados com 28,64% e tendo como último os viúvos, com apenas 2,55%.

Figura 6 - Percentual de registros de Fraude Eletrônica, ocorridos na Região Metropolitana de Belém, no período de 2021 a 2024, por Estado Civil da Vítima



Fonte: Construção do autor a partir de dados do SIAC (2025).

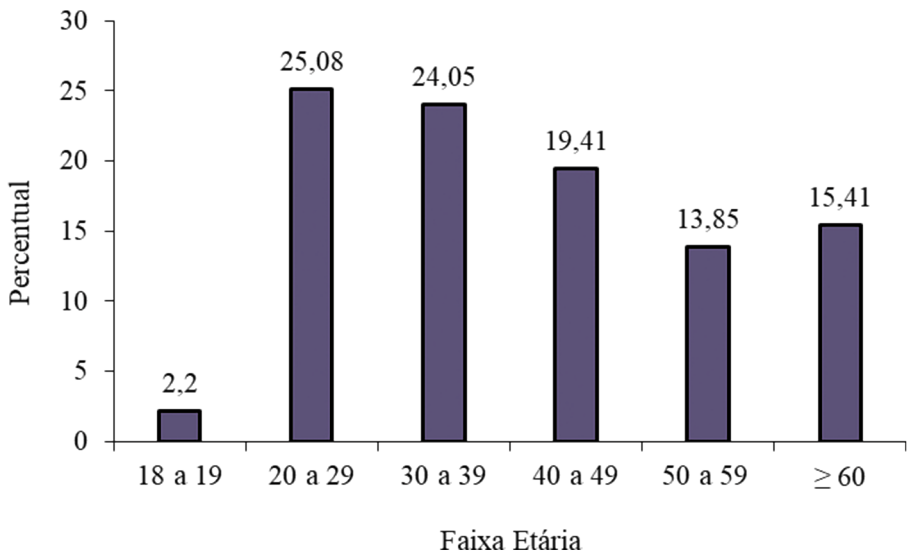
No caso do maior percentual, verificado entre solteiros ou solteiras, a literatura associa esse padrão ao maior uso declarado de aplicativos de relacionamento e redes sociais entre esse grupo. Silveira (2015) já havia destacado que a facilidade de acesso a tecnologias ampliou a incidência dos crimes virtuais que atingem múltiplas pessoas, de forma simultânea no ciberespaço.

No que se refere às vítimas que possuem relação conjugal, esse grupo soma quase 38% das vítimas e pode se enquadrar em modalidades de golpes que exploram o ambiente familiar, como o falso parente, em que criminosos solicitam dinheiro por aplicativos de mensagens instantâneas ou exploram vulnerabilidades familiares por meio da engenharia de urgência, induzindo as vítimas a fornecerem senhas e dados sensíveis de forma voluntária (Jesus; Milagre, 2016).

Nas categorias divorciados (6,04%) e viúvos (2,55%), embora possuam os menores percentuais estatísticos no presente estudo, guardam relevância para futuras investigações, pois a literatura associa esses grupos a modalidades de golpes sentimentais, nos quais os agressores constroem vínculo afetivo para explorar a carência emocional das vítimas (Souza, 2022). Estudos apontam esses grupos como alvos frequentes desse tipo de fraude, ainda que os dados da presente pesquisa não permitam confirmar predisposições psicológicas específicas. Cabe destacar, ainda, que o baixo número de registros nesses grupos pode estar associado à vergonha e ao abalo psicológico sofridos pelas vítimas, o que tende a reduzir a formalização da denúncia (Whitty, 2018).

No que se refere à faixa etária das vítimas (Figura 7), é possível verificar que as maiores faixas de incidência são de 20 a 29 anos com 25,08% e de 30 a 39 anos com 24,05% dos casos. Este fato pode ser atribuído ao uso intensivo de aplicativos de redes sociais, transações financeiras e plataformas de *e-commerce*, que facilitam o cotidiano com acesso à internet e outras ferramentas, porém expõem seus usuários aos riscos e vulnerabilidades exploradas por criminosos cibernéticos (Silveira, 2015).

Figura 7 - Percentual de registros de Fraude Eletrônica, ocorridos na Região Metropolitana de Belém, no período de 2021 a 2024, por Faixa Etária da Vítima



Fonte: Construção do autor a partir de dados do SIAC (2025).

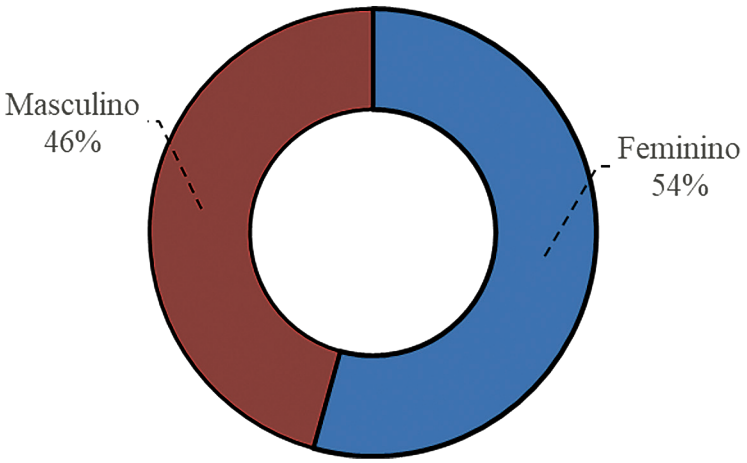
A continuidade nas demais faixas, de 40 a 49 anos, 19,41% e 50 a 59 anos, 13,85%, indica que a vitimização ocorre em todas as faixas da vida adulta tendo como fator de impacto, principalmente com relação aos crimes patrimoniais e a sua reconfiguração do *modus operandi*, acelerada pela Covid-19 e a migração em massa para o ambiente digital (Lima; Bueno, 2023).

No que se refere aos idosos (60 anos ou mais), o percentual apresentado foi de 15,41%, que embora esteja abaixo de outras faixas de adultos, este grupo é identificado pela literatura como hipervulnerável, dada a falta de familiaridade com a tecnologia e a confiança excessiva em mensagens falsas (Alves, 2023). Outros estudos indicam que *phishing* e falso funcionário (falsa central) são formas comuns que exploram a vulnerabilidade e o isolamento de pessoas idosas (Silva*et al.*, 2023).

O estudo do DataSenado (2024) revela a distribuição etária das vítimas semelhante à observada nesta pesquisa, principalmente no que se refere às faixas etárias de adultos e idosos. As faixas de 30 a 39 anos e 40 a 49 anos apresentaram percentuais próximos e elevados (23% e 20%, respectivamente). Nos grupos de 50 a 59 anos e iguais ou maiores de 60 anos, também houve aproximação de valores (14% e 16%), demonstrando a ausência de um perfil etário quando se trata de vitimização.

Em relação ao sexo da vítima (Figura 8), o estudo apresentou uma predominância maior entre as mulheres (54%) em relação ao homem (46%) entre as vítimas de fraude eletrônica e sua ocorrência na RMB, resultado que converge com estudos anteriores sobre maior incidência de mulheres entre vítimas de fraudes (Whitty, 2018).

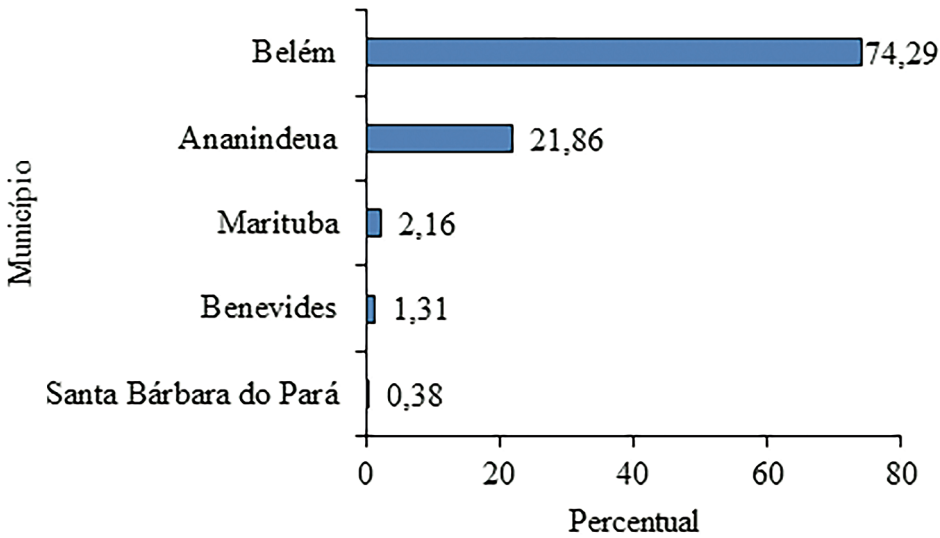
Figura 8 - Percentual de registros de Fraude Eletrônica, ocorridos na Região Metropolitana de Belém, no período de 2021 a 2024, por Sexo da Vítima



Fonte: Construção do autor a partir de dados do SIAC (2025).

Souza (2022) reforça que os crimes em razão do gênero não se restringem apenas a crimes contra a honra ou vingança pornográfica, mas atuam principalmente na violência patrimonial, como é o caso da fraude eletrônica em estudo, sendo diversa do mundo real, em que a violência física se torna a mais sofrida entre as mulheres. Silva e Azevedo (2022) e Nascimento (2024) também demonstraram uma maior incidência no público feminino nas questões relacionadas ao cibercrime, principalmente a tipologias específicas de fraude que se fundamentam em engenharia social, explorando vínculos afetivos e de confiança.

Figura 9 - Percentual de registros de Fraude Eletrônica, ocorridos na Região Metropolitana de Belém, no período de 2021 a 2024, por Município



Fonte: Construção do autor a partir de dados do SIAC (2025).

A análise espacial das ocorrências (Figura 9) revelou uma forte concentração na capital paraense, Belém, com cerca de 74,30% das ocorrências totais da Região Metropolitana, seguida por Ananindeua com 21,85%, enquanto os demais municípios apresentaram baixa participação, não somando 4%.

Pesquisadores como Adorno (2005) e Feltran (2018) identificaram que crimes urbanos contemporâneos estão fortemente associados aos principais centros de densidade populacional, dada a oferta de serviços bancários digitais e conectividade à internet. A concentração em núcleos urbanos maiores não é uma particularidade da capital paraense, mas fenômeno que se reproduz em escala nacional, conforme demonstram as análises do Anuário Brasileiro de Segurança Pública (FBSP, 2025), que apontou uma concentração de crimes digitais em regiões de maior densidade urbana e PIB.

3 CONSIDERAÇÕES FINAIS

Este artigo propôs analisar 21.813 boletins de ocorrência de fraude eletrônica registrados na Região Metropolitana de Belém (RMB) no período de 2021 a 2024, com dados fornecidos pela Secretaria de Inteligência e Análise Criminal (SIAC). A pesquisa adotou uma abordagem quantitativa descritiva, caracterizando o comportamento do fenômeno e o perfil sociodemográfico das vítimas.

Os resultados revelaram um crescimento exponencial das fraudes na RMB, com aumento de 1.202 casos em 2021 para 6.985 em 2024, representando uma expansão superior a 480% no período estudado. O maior salto se deu no período de 2021 a 2022, com crescimento de aproximadamente 410,65%, tendo como possíveis causas a pandemia de Covid-19, que acelerou a digitalização das transações financeiras, e a popularização do Pix como meio de transferência instantânea de valores. A partir de 2022, observou-se uma relativa estabilização nos patamares elevados, com o pico sendo observado em outubro de 2023.

Quanto à análise temporal, observou-se concentração em dias úteis com aproximadamente 85% das ocorrências, assim como os turnos, acumulados nos períodos diurnos com mais de 80% dos casos, observando-se que a concentração das ocorrências acompanha o horário convencional das instituições financeiras e as limitações de valores de transações estabelecidos.

A caracterização sociodemográfica das vítimas indica que a baixa escolaridade não é fator determinante para a maior suscetibilidade a golpes digitais, visto que 46% das vítimas iniciaram o ensino superior. No tocante ao gênero, observou-se maior proporção de mulheres entre as vítimas (54%), resultado convergente com outros estudos sobre vitimização feminina em fraudes eletrônicas.

Quanto à faixa etária, 49,13% das vítimas tinham entre 20 e 39 anos, faixa etária caracterizada pelo intenso uso de plataformas digitais, redes sociais e transações financeiras online. Todavia, o público idoso, com 60 ou mais anos de idade, representou 15,41% das ocorrências, grupo que a literatura descreve como potencialmente vulnerável em razão de menor familiaridade tecnológica, ainda que este estudo não tenha mensurado diretamente esse fator.

No estado civil, os solteiros constituíram a maioria absoluta (53,32%), seguidos de casados (28,64%), padrão associado à maior exposição digital

por meio de redes sociais e aplicativos de relacionamento. Houve grande diversidade profissional, com "outros" somando 55,21% dos casos, tendo como maiores índices os estudantes (8,07%), servidores públicos (5,15%), professores (4,64%), donas de casa (4,46%) e aposentados com 4,36%. Espacialmente, Belém concentrou 74,30%, seguida de Ananindeua com 21,85% dos casos, refletindo a maior densidade populacional e conectividade dos centros urbanos.

A análise dos dados indica que a ocorrência de fraudes eletrônicas acompanha as dinâmicas sociais e do sistema econômico formal, com concentração em dias e turnos de maior atividade comercial e financeira. A concentração das ocorrências nos dias da semana e horários comerciais é compatível com o aproveitamento de oportunidades estruturais da sociedade, conforme descrito por Misse (1997). O crescimento observado no período da análise acompanha a expansão de ferramentas de inclusão financeira, como o Pix, no mesmo intervalo temporal.

A diversidade do perfil das vítimas indica que a escolaridade, isoladamente, não é suficiente para explicar e justificar a exposição ao risco, sendo relevante considerar diversos outros fatores apontados como relevantes, como a exploração de gatilhos emocionais e urgências fabricadas apontada pela literatura consultada.

O estudo demonstra a necessidade de investimento nas investigações cibernéticas, com capacitação técnica continuada, aquisição de ferramentas que ampliem a atuação institucional e estabelecimento de protocolos de atuação em conformidade com a modalidade de fraude enfrentada. O enfrentamento eficaz do cibercrime, principalmente na modalidade da fraude eletrônica, exige acompanhamento constante com atuação integrada da legislação, tecnologia e políticas de segurança pública. Ainda se faz necessária uma atuação de divulgação e conscientização da sociedade com campanhas educativas que, com base nos dados apresentados, promovam o letramento digital para o uso adequado do ambiente virtual e menor exposição às fraudes eletrônicas e golpes cotidianos.

4 REFERÊNCIAS

ADORNO, S. **Crime e violência na sociedade brasileira contemporânea**. Jornal de Políticas Educacionais, Curitiba, v. 2, n. 4, p. 53-69, 2005.

ALCADIPANI, R.; LIMA, R. S.; BUENO, S. Estelionatos crescem, já superam os roubos e fortalecem o crime organizado no Brasil. In: Fórum Brasileiro de Segurança Pública. **18º Anuário Brasileiro de Segurança Pública**. São Paulo: FBSP, 2024. p. 96-105. Disponível em: https://publicacoes.forumseguranca.org.br/handle/123456789/253. Acesso em: 20 mar. 2025.

ALMEIDA, R. N. **Estelionato virtual no direito brasileiro**. 2023. 26 f. Trabalho de Conclusão de Curso (Graduação em Direito) - Escola de Direito, Negócios e Comunicação, Pontifícia Universidade Católica de Goiás, Goiânia, 2023.

ALVES, J. G. **Análise da prática do crime de fraude perpetrado por organizações criminosas e suas consequências no ambiente virtual**. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Faculdade de Educação, Universidade Federal de Mato Grosso do Sul, Campo Grande, 2023.

ARSAWATI, I. N. J.; DARMA, I. M. W.; ANTARI, P. E. D. A. Criminological Outlook of Cyber Crimes in Sexual Violence Against Children in Indonesian Laws. **International Journal of Criminology and Sociology**, **[S. l.]**, v. 10, p. 219–223, 2021. DOI: 10.6000/1929-4409.2021.10.26.

BACEN. Banco Central do Brasil. **Limites de valor para as transações Pix**. Brasília, DF: BCB, 2025. Disponível em: https://www.bcb.gov.br/meubc/faqs/p/limites-de-valor-para-as-transacoes-Pix. Acesso em: 10 jul. 2025.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. **Código Penal.** Brasília, DF: Senado Federal, 1940.

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.** Brasília, DF: Presidência da República, 2021.

BUSSAB, W. O.; MORETTIN, P. A. **Estatística básica**. 9.ed., São Paulo: Saraiva, 2017.

COSTA, V. B.; ABRANTES, J. S. A influência da Pandemia da COVID-19 nos crimes de estelionato digital ocorridos no Município de Santana-Amapá. **Revista Científica Multidisciplinar do CEAP,** v. 5, n. 1, 2023.

CRESPO, M. X. F. **Crimes digitais**. São Paulo: Saraiva, 2011.

DATASENADO. **Panorama Político 2024 - Apostas esportivas, golpes digitais e endividamento.** Senado Federal, Brasília, DF, set. 2024. Disponível em: https://www.senado.leg.br/institucional/datasenado/relatorio_online/pesquisa_aposta_esportiva/2024/interativo.html. Acesso em: 10 abr. 2025.

DOMINGOS, T. G.; JACOB, A. O Perfil do Criminoso nos Crimes Cibernéticos: Comportamentos, Motivações e Táticas**. Revista Multidisciplinar do Nordeste Mineiro**, **[S. l.]**, v. 10, n. 1, 2024.

FBSP. Fórum Brasileiro de Segurança Pública. **19º Anuário Brasileiro de Segurança Pública**. São Paulo/SP: FBSP, 2025.

FELTRAN, G. **Irmãos: uma história do PCC.** São Paulo: Companhia das Letras, 2018.

GIL, A. C. **Métodos e técnicas de pesquisa social**. 6. ed. São Paulo: Atlas, 2008.

IBGE. Instituto Brasileiro de Geografia e Estatística. Belém (PA) | **Cidades e Estados.** 2023

IBM SECURITY. **Cost of a Data Breach Report 2023**. IBM Security, 2023. Disponível em: https://www.ibm.com/downloads/cas/E3G5JMBP. Acesso em: 16 fev. 2024.

JESUS, D.; MILAGRE, J. A. **Manual de Crimes Informáticos**. São Paulo: Saraiva, 2016.

JUSTINIANO, N. F. **Terminologia e tecnologia: um estudo de termos de crimes cibernéticos.** 2017. 125 f. Dissertação (Mestrado em Linguística) – Universidade de Brasília, Brasília, 2017.

LIMA, A. C. V. F. A proteção de dados e a tecnologia criptográfica: um duelo entre o poder público e a preservação da privacidade. In: LOPES FILHO, João Herculino de Souza (org.). **Crimes Digitais**. Brasília: UniCEUB/ICPD, p. 146-169, 2020.

LIMA, R. S.; BUENO, S. As novas configurações dos crimes patrimoniais no Brasil. In: Fórum Brasileiro de Segurança Pública. **17º Anuário Brasileiro de Segurança Pública**. São Paulo: FBSP, 2023.

LOPES, M. P.; LOPES, J. A. B. Crimes virtuais no ordenamento jurídico brasileiro. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, São Paulo, v. 9, n. 8, p. 462-472, ago. 2023.

MISSE, Michel. **Crime urbano, sociabilidade violenta e ordem legítima.** Comentários sobre as hipóteses de Machado da Silva. Mimeo. Rio de Janeiro, 1997.

MONTEIRO, J. R. da C.; RAMOS, E. M. L.S. Caracterização estatística dos crimes patrimoniais virtuais no Estado do Pará. In: RAMOS, Edson Marcos Leal Soares; MONTEIRO, José Ramon da Conceição (org.). **Segurança Pública**: desenvolvimento em ensino, pesquisa e extensão. v. 1. Londrina: Santa Cruz, 2021

NASCIMENTO, F. B. **Aplicativo Game Phishing: uma proposta de tecnologia para mitigar os golpes virtuais motivados por phishing** 2024. Dissertação (Mestrado em Segurança Pública). Programa de Pós-Graduação em Segurança Pública. Instituto de Filosofia e Ciências Humanas. Universidade Federal do Pará, Belém, Pará, Brasil, 2024.

NERY, C.; BRITTO, V. **Internet já é acessível em 90,0% dos domicílios do país em 2021**. Agência IBGE Notícias, 2022. Disponível em: https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/34954-internet-ja-e-acessivel-em-90-0-dos-domicilios-do-pais-em-2021. Acesso em: 20 out. 2025.

OLIVEIRA, E. P. de; BRITO, P. L. P. de; FERREIRA JÚNIOR, A. C. O aumento do estelionato digital em tempos pandêmicos. **Graduação em Movimento-Ciências Jurídicas**, v. 3, n. 1, p. 61-77, 2024.

ROZA, R. H. Revolução informacional e os avanços tecnológicos da informática e das telecomunicações. **Ciência da Informação em Revista**, v. 4, n. 3, p. 03-11, 2017.

SANTORO, F. M.; REVOREDO, K. C.; BAIÃO, F. A. (org.). **Impacto social das novas tecnologias**. 1.ed., Cuiabá: EdUFMT Digital, 2020.

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

SILVA, D. B. da; ALMEIDA, A. C. de; VALENÇA, C. S. A. A.; FURTADO, C. A. M.; VASCONCELOS, H. M. B. de; TRAJANO, L. A.; ARAUJO, M. V. de; FURTADO, B. M. A. S. M. Cibercrimes Sob a Perspectiva Científica: Revisão Integrativa da Produção Nacional e Internacional. **ARACÊ** , **[S. l.]**, v. 7, n. 8, p. e7643, 2023.

SILVA, L. C.; AZEVEDO, D. G. de. Balanço dos principais crimes cibernéticos ocorridos no município de Belém/PA no período de 2018 a 2020**. Research, Society and Development**, v. 11, n. 1, 2022.

SILVEIRA, B. O. **A Violência na Prática de Crimes no Ciberespaço**. 2015. 110 f. Dissertação (Mestrado em Segurança Pública) – Programa de Pós-Graduação em Segurança Pública, Universidade Federal do Pará, Belém, Brasil, 2015.

SOUZA, F. M. **Sextorsão e Romance Scam no Estado do Pará**. 88f. Dissertação (Mestrado em Segurança Pública). Programa de Pós-Graduação em Segurança Pública, Instituto de Filosofia e Ciências Humanas, Universidade Federal do Pará, Belém, Pará, Brasil 2022.

SYDOW, S. T. **Curso de Direito Penal Informático**. 3. ed. Salvador: JusPodivm, 2022.

WHITTY, M. T. Do You Love Me? Psychological Characteristics of **Romance Scam** Victims. **Cyberpsychology, Behavior, and Social Networking**, v. 21, n. 2, 2018.

ZACARIAS, F.; FREIRE, L. Z. Crimes virtuais: análise das dificuldades e limitações ao combate. **Revista Jures**, v. 16, n. 29, p. 29-61, 2023.

Data da submissão: 12.03.2026.

Data da aprovação: 22.06.2026.