

CRIMES DE ESTELIONATO DIGITAL CONTRA IDOSOS NO BRASIL: VULNERABILIDADE, PREVENÇÃO E RESPONSABILIZAÇÃO JURÍDICA

Vanessa Daiani Vieira Gonçalves¹

Augusto Martins de Jesus²

RESUMO: estelionato digital contra idosos tem se intensificado no Brasil em razão da combinação entre avanços tecnológicos, falhas na proteção de dados e a hipervulnerabilidade característica da pessoa idosa no ambiente digital. Este artigo analisa as modalidades de golpes mais recorrentes, os impactos financeiros, psicológicos e sociais sofridos pelas vítimas e os fatores estruturais que favorecem a expansão desse fenômeno. A partir de abordagem qualitativa, exploratória e bibliográfica, são examinados dispositivos legais, estudos acadêmicos, relatórios técnicos e contribuições interdisciplinares das áreas do Direito, da Sociologia da Tecnologia e dos Estudos da Longevidade. Os resultados demonstram que as fraudes digitais não decorrem de ingenuidade individual, mas de vulnerabilidades sistêmicas agravadas por vazamentos massivos de dados e por técnicas de engenharia social altamente sofisticadas. Revela-se, ainda, que os mecanismos de responsabilização penal, civil e administrativa, embora existentes, enfrentam limitações na prática investigativa e na efetividade da proteção informacional.

Palavras-chave: estelionato digital; idosos; engenharia social; vazamento de dados; vulnerabilidade digital; crimes cibernéticos

INTRODUÇÃO

O avanço acelerado das tecnologias digitais nas últimas décadas transformou de forma profunda as relações sociais, econômicas e comunicacionais, produzindo novas oportunidades e múltiplos riscos relacionados à segurança da informação. Entre esses riscos, destaca-se a expansão do estelionato digital, prática que mobiliza técnicas cada vez mais sofisticadas de engenharia social, usurpação de identidade, manipulação psicológica e exploração de dados pessoais. No Brasil, tal fenômeno atinge com especial intensidade a população idosa, grupo reconhecido pelo ordenamento jurídico e pelos estudos sociais como hipervulnerável no ambiente digital. Nesse contexto, o presente artigo tem como objeto de pesquisa a análise das modalidades de estelionato digital que incidem sobre idosos no Brasil, considerando suas causas, seus impactos multidimensionais e os mecanismos jurídicos disponíveis para enfrentamento, prevenção e responsabilização.

¹ Graduanda em Direito pela Fundação Educacional de Fernandópolis (FEF). E-mail: gabsmaciel1913@gmail.com

² Professor da Fundação Educacional de Fernandópolis (FEF), onde atua como orientador acadêmico. Mestre em Jornalismo pela Universidade Estadual de Ponta Grossa. Bacharel em Jornalismo pela Universidade do Estado de Minas Gerais, em Direito pelo Centro Universitário de Votuporanga (Unifev) e em Publicidade e Propaganda pela Cruzeiro do Sul Virtual (Universidade de Franca – Unifran). Especialista em Lei Geral de Proteção de Dados e em Direito Público (Faculdade Legale). E-mail: augustodejesus@fef.edu.br

A relevância social dessa investigação decorre não apenas da alta incidência de golpes contra idosos, mas dos efeitos amplos e profundos que tais fraudes provocam na vida dessas vítimas. Além das perdas patrimoniais, os golpes produzem sofrimento emocional, abalo psicológico, rupturas familiares, retração social e comprometimento da autonomia. Do ponto de vista social, trata-se de uma problemática que expõe falhas sistêmicas de alfabetização digital, deficiência na proteção de dados, fragilidade de políticas públicas e ineficiência estrutural na resposta estatal, especialmente no campo investigativo. No plano acadêmico e científico, a relevância reside na necessidade de produzir análises transdisciplinares, articulando Direito Penal, Direito do Consumidor, LGPD, Sociologia da Tecnologia e Estudos da Longevidade, capazes de compreender o fenômeno de forma ampla e integrada. O caráter contínuo de atualização normativa reforça a pertinência da pesquisa, especialmente em um cenário de criminalidade cibernética em expansão.

É a partir desse cenário que emerge a problematização central deste estudo: por que o estelionato digital tem se expandido de forma tão contundente entre a população idosa no Brasil e quais fatores (tecnológicos, sociais, estruturais e jurídicos) contribuem para a intensificação dessa vulnerabilidade? Além disso, de que modo os mecanismos legais disponíveis, aliados a estratégias sociais e institucionais, podem oferecer resposta efetiva a esse quadro, considerando as especificidades da pessoa idosa e as particularidades da criminalidade cibernética contemporânea? É essa questão que orienta o percurso analítico do artigo e permite compreender a complexidade do fenômeno estudado.

A partir dessa problematização, a pesquisa apresenta um objetivo geral: examinar o fenômeno do estelionato digital contra idosos no Brasil, suas modalidades, seus impactos e o arcabouço jurídico destinado ao enfrentamento. Como objetivos específicos, busca-se: analisar as bases conceituais e sociotecnológicas do estelionato digital; identificar as principais modalidades de golpes praticados contra idosos; compreender os impactos financeiros, psicológicos e sociais sofridos pelas vítimas; discutir estratégias de prevenção e proteção digital; e (e) examinar os mecanismos jurídicos de responsabilização penal, civil, administrativa e consumerista.

No que se refere à metodologia, o estudo adota abordagem qualitativa, exploratória e bibliográfica, fundamentada em legislação, doutrina, artigos científicos, relatórios técnicos de instituições especializadas e documentos oficiais relacionados à proteção da pessoa idosa e ao enfrentamento da criminalidade cibernética. Trata-se de pesquisa baseada em fontes secundárias, com análise teórico-interpretativa e diálogo interdisciplinar entre Direito, Sociologia da Tecnologia e Estudos da Longevidade.

A estrutura do artigo foi organizada em três capítulos, de forma a garantir coerência metodológica e progressão lógica. A primeira parte apresenta as bases conceituais, normativas e tecnológicas do estelionato digital, discutindo sua evolução jurídica, as técnicas de engenharia social utilizadas pelos criminosos, as principais modalidades de golpes e o papel dos vazamentos massivos de dados como fator estruturante da vulnerabilidade. A segunda parte aprofunda a análise dos impactos sofridos pelos idosos e apresenta estratégias de prevenção que envolvem educação digital, apoio familiar, corresponsabilidade institucional e políticas públicas. A última parte, por sua vez, sistematiza os mecanismos jurídicos de responsabilização penal, civil, administrativa e consumerista, discutindo decisões jurisprudenciais e avaliando limites e avanços na proteção jurídica da pessoa idosa.

1. ESTELIONATO DIGITAL CONTRA IDOSOS: FUNDAMENTAÇÃO CONCEITUAL, CARACTERÍSTICAS TECNOLÓGICAS E MODALIDADES DE FRAUDES

A primeira seção tem por finalidade estabelecer as bases conceituais, jurídicas e sociotécnicas necessárias para a compreensão do estelionato digital como fenômeno criminal complexo, destacando suas particularidades no contexto da sociedade informacional contemporânea. A análise parte da definição legal do estelionato e avança para sua reconstrução teórica diante das transformações tecnológicas recentes, que ampliaram as formas de interação digital e criaram dinâmicas de manipulação fraudulenta.

A seção busca demonstrar que a violência praticada contra idosos em ambiente digital não decorre apenas de condutas individuais, mas de um ecossistema caracterizado pela rápida evolução tecnológica, pela fragilidade dos sistemas de proteção de dados e pela hipervulnerabilidade de grupos específicos. Para isso, articula-se um percurso analítico que combina Direito Penal, Sociologia das Tecnologias e estudos sobre envelhecimento, oferecendo um panorama que evidencia a necessidade de interpretação ampliada do fenômeno. Para isso, o capítulo se estrutura em quatro eixos: evolução normativa, engenharia social, modalidades de golpes e impactos estruturais de vazamentos de dados pessoais.

1.1. Estelionato digital e sua evolução normativa: fundamentos jurídicos, aspectos tecnológicos, vulnerabilidades associadas e desafios contemporâneos

O estelionato digital, enquanto fenômeno jurídico e sociotécnico, representa uma das expressões mais complexas da criminalidade contemporânea. Embora o artigo 171 do Código Penal Brasileiro já prevísse, desde sua formulação original, o núcleo essencial da conduta, ou seja, induzir alguém em erro mediante artifício ou ardil, o avanço das tecnologias de informação transformou o modo como esse crime se manifesta, gerando novas formas de manipulação, ocultação e interação entre criminoso e vítima. Essa transformação decorre, sobretudo, da crescente digitalização das práticas sociais, bancárias, previdenciárias e comunicacionais, que ampliou o espaço operacional dos cibercriminosos.

Como explica Castells (2003), a sociedade em rede redefine relações de poder, informação e vulnerabilidade: indivíduos tecnologicamente menos preparados tornam-se alvos preferenciais de manipulações digitais. No contexto brasileiro, essa vulnerabilidade é intensificada pelas desigualdades sociais, pela exclusão digital e pelo ritmo acelerado de adoção de tecnologias sem adequada alfabetização digital, especialmente entre idosos.

Diante dessas mudanças, a Lei nº 14.155/2021 buscou atualizar o arcabouço normativo, introduzindo qualificadoras para fraudes realizadas por meios eletrônicos. A pena, antes restrita a reclusão de 1 a 5 anos, passou para 4 a 8 anos, quando utilizada engenharia social via redes sociais, e-mails, ligações ou aplicativos. O legislador reconheceu que o ambiente digital cria condições que aumentam o risco dos crimes e dificultam a persecução penal, especialmente quando o criminoso utiliza servidores no exterior ou mecanismos de anonimização, o que enseja aumento de pena de até dois terços.

A proteção jurídica torna-se ainda mais relevante quando o crime envolve idosos, população historicamente reconhecida pelo ordenamento como hipervulnerável. Serra et al. (2025) afirmam que o idoso experimenta vulnerabilidade digital cumulativa: combina declínio cognitivo, limitações tecnológicas, aprendizagem digital tardia e, muitas vezes, isolamento social. Por isso, o §4º do art. 171 prevê aumento de pena de até o dobro.

Ocorre que, mesmo com avanços legislativos, pesquisadores como Costa (2025) e Button (2025) apontam que a legislação permanece “correndo atrás” das inovações tecnológicas. A velocidade de atualização dos cibercriminosos supera a atualização normativa e institucional, gerando lacunas regulatórias. A ausência de tipificações penais específicas para vazamento de dados, por exemplo, apesar da LGPD, fragiliza a resposta estatal.

Além disso, há desafios investigativos decorrentes do uso de bots, VPNs, spoofing telefônico e ferramentas que mascaram geolocalização. Como observa Santos & Wojahn (2022), a investigação de crimes digitais exige infraestrutura altamente especializada, nem sempre disponível em delegacias tradicionais, o que facilita a impunidade.

Assim, compreender o estelionato digital exige uma abordagem transdisciplinar que articule Direito Penal, Sociologia, Segurança da Informação e Estudos da Longevidade. Trata-se de um fenômeno em franca expansão, exigindo constante atualização legislativa e políticas preventivas consistentes.

1.2. Particularidades do estelionato digital: engenharia social, tecnologias de ocultação, dinâmicas psicológicas e vulnerabilidades cognitivas exploradas pelos criminosos

O sucesso³ do estelionato digital não decorre apenas do uso de ferramentas tecnológicas, mas, sobretudo, da capacidade dos criminosos de manipular elementos emocionais, cognitivos

³ O termo sucesso, embora habitualmente associado a resultados positivos, é empregado aqui em sentido técnico-descritivo, para indicar a capacidade de determinada prática criminosa alcançar seus objetivos ilícitos. No campo da criminologia, a expressão não possui conotação valorativa, mas indica que o delito prospera e se torna eficaz em ambientes marcados por vulnerabilidades sociais, emocionais e tecnológicas.

e relacionais da vítima. Essa técnica, conhecida como engenharia social, consiste na utilização de estratégias psicológicas cuidadosamente planejadas para explorar emoções humanas, confiança, medo, urgência, afeição, insegurança, ignorância técnica, com o objetivo de induzir comportamentos prejudiciais.

Recuero (2021) enfatiza que a engenharia social opera na interseção entre tecnologia e afetos: o criminoso utiliza ferramentas digitais para ativar gatilhos emocionais que diminuem o senso crítico da vítima. No caso de idosos, essa vulnerabilidade é amplificada por fatores como: (a) confiança maior em solicitações supostamente oficiais; (b) dificuldade de identificar sinais de fraude digital; (c) receio de parecer ignorante perante interlocutores; (d) solidão emocional, que aumenta receptividade a mensagens de afeto; (e) menor fluência em leitura digital, dificultando verificação de autenticidade.

Pesquisadores como Button (2025) e Costa (2025) afirmam que idosos constituem o principal alvo de golpes em escala internacional. Nos Estados Unidos, o *Elder Fraud Annual Report* do FBI (2024) mostra que vítimas com mais de 60 anos representam quase metade das perdas financeiras totais relacionadas a golpes online. No Brasil, conforme o Fórum Brasileiro de Segurança Pública (2023), mais de 70% dos registros envolvendo pessoas acima de 60 anos estão associados a fraudes digitais e engenharia social.

Do ponto de vista técnico, a engenharia social é potencializada por recursos como: spoofing telefônico (simulação de números oficiais), criação de perfis falsos com fotografias reais, manipulação de metadados, uso de deepfakes, bots automatizados, mensagens sequenciais preparadas previamente etc.

Santos & Wojahn (2022) argumentam que, diferentemente de ataques puramente tecnológicos (como malwares), a engenharia social explora vulnerabilidades humanas, e, portanto, a proteção depende tanto de educação digital quanto de políticas sociais e culturais. Do ponto de vista cognitivo, estudos de longevidade mostram que o envelhecimento natural reduz a velocidade de processamento de informações, a capacidade de avaliar riscos rapidamente e a habilidade de identificar inconsistências linguísticas, todos fatores que ampliam a vulnerabilidade ao golpe. Assim, as particularidades do estelionato digital não se limitam à tecnologia utilizada, mas incluem uma compreensão profunda dos processos emocionais que envolvem a vítima, exigindo respostas jurídicas e sociais amplas.

1.3. Modalidades de golpes digitais contra idosos: fundamentação científica, recorrência estatística e caracterização criminológica das principais práticas fraudulentas.

As modalidades de golpes, golpe do falso parente, falso funcionário de banco, phishing, falsas promoções, romance scam, golpes do INSS, clonagem de WhatsApp etc., não são percepções empíricas, mas categorias amplamente reconhecidas na literatura científica, na criminologia digital e nos relatórios de instituições especializadas.

Segundo o relatório SaferNet Brasil 2023–2024, golpes de engenharia social direcionados a idosos compõem 31% das denúncias analisadas, sendo o golpe do falso parente (“Golpe do WhatsApp”) o mais recorrente. O CIDCIBER/Polícia Federal (2024) classifica golpes contra idosos em quatro grandes categorias: (a) golpes de identidade social (falso parente, romance scam); (b) golpes financeiros (falso funcionário de banco, empréstimos consignados); (c) golpes tecnológicos (phishing, clonagem de aplicativos, invasão de contas); (d) golpes institucionais (falsos servidores do INSS, saúde, bancos).

Mendonça (2023) demonstra que o golpe do falso funcionário de banco apresenta crescimento exponencial entre idosos, pois se baseia na autoridade percebida da instituição financeira, gerando forte confiabilidade. O idoso, temendo prejuízos ou bloqueios, tende a obedecer prontamente às instruções fraudulentas.

No caso do *romance scam*, Button (2025) afirma que idosos representam o grupo com maior impacto emocional e financeiro, pois os criminosos constroem relações afetivas prolongadas antes de solicitar transferências. Estudos internacionais demonstram perdas que chegam a milhões de dólares por vítima idosa, devido à manipulação emocional profunda.

O phishing, segundo Recuero (2021), permanece como uma das ferramentas mais eficazes de coleta de dados, pois se apoia na imitação de estética institucional, dificultando a distinção entre mensagens legítimas e fraudes. Idosos, com menor prática no reconhecimento de elementos digitais, tornam-se alvos preferenciais.

A clonagem de WhatsApp, conforme relatado pelo CERT.br (2024), consolidou-se como uma das maiores ameaças no Brasil nos últimos anos. O método utiliza engenharia social para obtenção do código de verificação, após o que o criminoso assume o perfil da vítima e solicita valores a familiares, golpe geralmente bem-sucedido quando envolve idosos.

Os golpes envolvendo INSS, por sua vez, são largamente registrados no Ministério da Previdência (2023), que aponta tentativas de fraude envolvendo “liberação de benefícios”, “bloqueio de aposentadorias” e “atualização cadastral”, manipulando a preocupação do idoso com seu sustento.

A literatura demonstra ainda que pirâmides financeiras atraem idosos pela promessa de segurança e retorno rápido, conforme analisado por Button (2025), que classifica esses esquemas como fraudes capazes de destruir patrimônio acumulado ao longo de décadas. Assim, todas as modalidades listadas possuem lastro científico, frequência comprovada e relevância criminológica, justificando plenamente sua presença no artigo.

1.4. Estelionato digital e vazamento massivo de dados pessoais: a Operação Tatu Canastra e a construção de um cenário de vulnerabilidade estrutural

A fragilidade digital da população idosa é aprofundada por falhas sistêmicas no tratamento de dados pessoais no Brasil, como demonstrado pela Operação Tatu Canastra, deflagrada pela Polícia Civil de São Paulo em 2024. A operação revelou uma organização criminosa especializada no vazamento, comercialização e enriquecimento de dados sensíveis pertencentes a mais de 120 milhões de brasileiros, provenientes de bancos digitais, prefeituras, concessionárias de telefonia, autarquias previdenciárias e plataformas de serviços.

Segundo o relatório da Polícia Civil, os criminosos alimentavam um banco de dados clandestino atualizado em tempo real, contendo CPF, endereço, renda, score financeiro, dados bancários, vínculos empregatícios, histórico de crédito, informações de saúde e registros previdenciários. Esse “perfil comportamental” permitia a personalização dos golpes praticados, especialmente contra idosos, alvo preferencial pela facilidade de manipulação.

Figura 1. Operação da Polícia Civil do interior de SP investiga grupo responsável por vazamento de dados de milhões de brasileiros



Fonte: Portal G1 / Polícia Civil/Divulgação, 2024.

Button (2025) explica que esse cenário representa um fenômeno conhecido na literatura como fraude por perfis enriquecidos, no qual criminosos utilizam dados reais da vítima para construir narrativas altamente convincentes, ampliando a taxa de sucesso das fraudes. Trata-se de prática que une vazamento de dados, engenharia social e estrutura criminal organizada.

Do ponto de vista da LGPD, esse episódio revela falhas graves de segurança tanto em órgãos públicos quanto em empresas privadas, configurando incidentes de alto risco. Como aponta Costa (2025), o vazamento de dados sensíveis não prejudica apenas a privacidade, mas cria condições para crimes financeiros de grande impacto, especialmente contra grupos vulneráveis.

Além disso, a operação demonstra que a vulnerabilidade do idoso decorre de limitações individuais e de falhas sistêmicas: ausência de investimentos em segurança da informação, práticas negligentes de armazenamento, fragilidade na criptografia, falta de transparência no tratamento de dados e ausência de responsabilização efetiva de controladores.

Esse contexto mostra que o estelionato digital contra idosos deve ser entendido como problema coletivo, não individual. O idoso é vítima final de uma cadeia de eventos que começa no vazamento estatal ou privado e culmina em manipulação emocional extremamente sofisticada. Por isso, políticas de prevenção, responsabilização e educação digital devem ser integradas e contínuas.

2. IMPACTOS DO ESTELIONATO DIGITAL CONTRA IDOSOS E O PAPEL DAS ESTRATÉGIAS DE PREVENÇÃO NO ENFRENTAMENTO À VULNERABILIDADE DIGITAL

Neste momento, a pesquisa aprofunda a análise dos impactos produzidos pelo estelionato digital na vida de pessoas idosas, deslocando o foco do marco normativo para a experiência concreta das vítimas. Essa escolha metodológica permite compreender o crime para além de sua dimensão jurídico-penal, destacando seus efeitos sociais, psicológicos, econômicos e relacionais. A intenção é demonstrar que o golpe digital, embora tecnicamente sofisticado, opera fundamentalmente pela fragilidade cognitiva e emocional da pessoa idosa, resultando em danos que ultrapassam o prejuízo financeiro.

Além de examinar os impactos multidimensionais, o presente capítulo discute estratégias de prevenção e proteção, evidenciando que o enfrentamento dessa modalidade criminosa depende de ações integradas entre Estado, família, instituições financeiras, empresas de tecnologia e políticas públicas de alfabetização digital. A análise reforça que a vulnerabilidade não é atributo individual do idoso, mas produto de um ambiente que frequentemente negligencia segurança informacional, educação tecnológica e acompanhamento social. Os intertítulos seguintes desenvolvem, de forma articulada, esses dois grandes eixos: os impactos sociais e a construção de mecanismos preventivos.

2.1. Impactos financeiros, psicológicos e sociais do estelionato digital em idosos: uma análise multidimensional da vulnerabilidade e de seus efeitos estruturais

O estelionato digital praticado contra idosos não pode ser compreendido apenas como um delito patrimonial. Trata-se de um fenômeno de natureza multidimensional, que produz impactos profundos e interligados nas esferas econômica, emocional, social e até mesmo na saúde física desse grupo populacional. Estudos apontam que os efeitos do golpe extrapolam o prejuízo financeiro, atingindo dimensões subjetivas que comprometem a autonomia, o senso de segurança e a autoestima do idoso (OLIVEIRA, 2021; SANTOS & WOJAHN, 2022).

No plano econômico, o prejuízo financeiro tende a ser devastador. Uma parte significativa dos idosos vive de aposentadoria, pensão ou recursos acumulados ao longo da vida, meios que, quando subtraídos, podem comprometer necessidades básicas como aquisição de medicamentos, alimentação, cuidados médicos e moradia. Segundo o Fórum Brasileiro de Segurança Pública (2022–2023), perdas decorrentes de fraudes digitais contra idosos cresceram mais de 60% nos últimos dois anos, evidenciando a escalada desse tipo de vitimização.

Esse impacto econômico se conecta a sentimentos de culpa, vergonha e autodepreciação, conforme apontam estudos de longevidade e psicogerontologia (NERI, 2019; COSTA, 2025). Isso ocorre porque o idoso, ao perceber que foi enganado, frequentemente interpreta o golpe como fracasso pessoal, e não como consequência de manipulações altamente sofisticadas. Tal percepção, ainda que equivocada, produz sofrimento emocional significativo e pode desencadear quadros de ansiedade, insônia, perda de apetite, estresse crônico e sintomas depressivos.

Do ponto de vista social, muitos idosos passam a desconfiar de interações digitais e presenciais, reduzindo sua participação em atividades online e diminuindo o contato virtual com familiares, principalmente em contextos onde o golpe envolveu falsos parentes ou perfis clonados. A retração digital compromete a inclusão tecnológica do idoso, afastando-o de ferramentas que poderiam ampliar sua autonomia, como serviços bancários online, telemedicina e acesso remoto a políticas sociais (CASTELLS, 2003; RECUERO, 2021).

Há também impactos na dinâmica familiar. Em muitos casos, a família reage com irritação ou surpresa, reforçando o sentimento de culpa da vítima. Como observa o relatório Elder Fraud 2024 (FBI), idosos vítimas de fraude tendem a esconder a situação, o que dificulta a denúncia, agrava o isolamento e aumenta a reincidência da vitimização.

Além disso, a perda de recursos financeiros pode gerar dependência econômica da família, gerando tensões, conflitos e até negligência. Estudos da área de Serviço Social destacam que a dependência econômica forçada, decorrente de golpes, pode alterar relações de cuidado, criar sobrecarga para os familiares e afetar a dignidade do idoso (SERRA et al., 2025).

O estelionato digital, portanto, não se limita a uma fraude econômica. Ele altera a maneira como o idoso se percebe no mundo digital, rompe vínculos sociais, produz consequências psicológicas duradouras e aprofunda vulnerabilidades pré-existentes. Em uma sociedade que avança rapidamente rumo à digitalização, compreender esses impactos é indispensável para formular políticas de prevenção e proteção eficazes.

2.2. Estratégias de prevenção e proteção digital: educação tecnológica, apoio familiar, políticas públicas e corresponsabilidade institucional

O enfrentamento ao estelionato digital exige uma abordagem articulada entre alfabetização digital, políticas públicas, responsabilidade institucional e suporte familiar. A prevenção é reconhecida pela literatura como a principal ferramenta para reduzir a vitimização

de idosos, sobretudo porque este grupo se encontra em posição de vulnerabilidade digital estrutural (MORAES, 2019; BUTTON, 2025).

O primeiro eixo dessa prevenção é a educação digital, que deve ir além do ensino de operações básicas. Ela deve incluir formação crítica sobre reconhecimento de tentativas de fraude, análise de veracidade de mensagens, uso de autenticação multifatorial e práticas de privacidade digital. Programas de capacitação podem ser implementados por universidades, centros de convivência e órgãos públicos, conforme sugerem pesquisas em políticas de envelhecimento (NERI, 2019; SERRA et al., 2025). Estudos mostram que idosos que participam de cursos de alfabetização digital reduzem em mais de 40% a probabilidade de cair em golpes (SaferNet, 2024). Entretanto, a prevenção não se limita ao idoso. A família desempenha papel essencial na criação de uma rede de proteção. Comunicação constante, acompanhamento de operações bancárias, revisão conjunta de mensagens suspeitas e apoio emocional após tentativas de golpe constituem práticas fundamentais. Como destaca SANTOS & WOJAHN (2022), a família é o primeiro núcleo de proteção, e sua atuação reduz drasticamente a incidência de fraudes.

As instituições financeiras, empresas de telefonia, plataformas digitais e órgãos públicos têm igualmente responsabilidades. O CDC, a LGPD e resoluções do Banco Central impõem deveres de segurança, transparência e cuidado com dados pessoais. A implementação de sistemas antifraude mais robustos, biometria avançada, monitoramento de transações atípicas e atendimento especializado ao idoso são medidas recomendadas por Mendonça (2023) e Costa (2025). No plano estatal, campanhas públicas de conscientização desempenham função crucial. A Constituição Federal, em seu artigo 230, atribui à família, à sociedade e ao Estado o dever de amparar o idoso, garantindo dignidade, bem-estar e participação comunitária. Políticas públicas de prevenção a fraudes devem integrar princípios constitucionais, a Política Nacional do Idoso e os mecanismos previstos no Estatuto do Idoso.

Outro aspecto relevante é o fortalecimento das Delegacias Especializadas em Crimes Cibernéticos e a ampliação de equipes de perícia digital. Sem capacidade investigativa adequada, a prevenção perde efetividade e os crimes permanecem impunes, incentivando sua propagação. Assim, as estratégias de prevenção ao estelionato digital precisam atuar em quatro dimensões simultâneas⁴: (1) educação e alfabetização digital; (2) apoio e acompanhamento

⁴ As quatro dimensões aqui apresentadas resultam de uma síntese construída ao longo do desenvolvimento da pesquisa, a partir da análise do material teórico e empírico coletado. Não se trata, portanto, de um modelo previamente consolidado ou consensual na literatura, mas de uma proposta interpretativa formulada por esta autora com base nas evidências examinadas, visando oferecer caminhos possíveis de intervenção e prevenção no contexto do estelionato digital contra idosos.

familiar; (3) responsabilidade institucional e proteção de dados; e, por fim, (4) atuação estatal coordenada e políticas públicas de conscientização. Somente uma abordagem integrada pode reduzir de forma consistente a vitimização de idosos e promover inclusão digital segura.

3. BASE NORMATIVA E MECANISMOS DE RESPONSABILIZAÇÃO NOS CRIMES DE ESTELIONATO DIGITAL CONTRA IDOSOS: ANÁLISE PENAL, CIVIL, ADMINISTRATIVA E INTERPRETAÇÕES JURISPRUDENCIAIS

A terceira e última seção deste trabalho adota uma abordagem jurídico-normativa para examinar os mecanismos de responsabilização aplicáveis aos crimes de estelionato digital contra idosos, articulando os planos penal, civil, administrativo e consumerista. Seu objetivo é demonstrar que a proteção jurídica da pessoa idosa depende de um conjunto interdependente de normas, que inclui desde a tipificação penal da conduta até a responsabilidade objetiva de instituições financeiras e a observância rigorosa das obrigações impostas pela Lei Geral de Proteção de Dados.

Essa parte cumpre um papel essencial na metodologia da pesquisa: conecta a análise conceitual e social desenvolvida nos capítulos anteriores ao marco jurídico que fundamenta as respostas institucionais ao fenômeno. Ao sistematizar a legislação aplicável, reunir interpretações jurisprudenciais relevantes e discutir os limites e potencialidades de cada esfera de responsabilização, o capítulo fornece ao leitor um panorama completo da arquitetura normativa vigente. Assim, permite compreender “o que é” o estelionato digital, “quais impactos causa” e “como o Direito responde” a essa realidade.

3.1. A estrutura jurídico-penal do estelionato digital: análise do art. 171 do Código Penal, agravantes específicas contra idosos, dificuldades investigativas e tensões produzidas pela Lei 14.155/2021

O estelionato digital ocupa posição central no debate contemporâneo sobre criminalidade cibernética e proteção penal de grupos vulneráveis. O artigo 171 do Código Penal Brasileiro, ao definir o crime de estelionato, estabelece como núcleo da conduta “obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil ou qualquer outro meio fraudulento”. Embora essa definição tenha sido suficiente por décadas, o avanço da tecnologia expôs lacunas na adequação normativa para lidar com fraudes perpetradas em ambiente digital.

Com o crescimento das interações virtuais, sobretudo após 2020⁵, o legislador promulgou a Lei nº 14.155/2021, que modernizou o dispositivo penal e introduziu qualificadoras específicas para o estelionato cometido “por meio de relação eletrônica ou telefônica, redes sociais, aplicativos, ou qualquer outro meio fraudulento semelhante”. Essa inovação reconhece a mudança de cenário criminal e eleva a pena para reclusão de 4 a 8 anos, além de multa, nos casos de fraude efetivada mediante engenharia social, manipulação tecnológica ou falsificação de identidade digital.

Outro ponto fundamental da Lei 14.155/2021 é o aumento de pena quando o agente utiliza servidores de informática mantidos no exterior ou mecanismos que dificultem a identificação da origem do delito. Isso se relaciona diretamente à natureza transnacional dos crimes cibernéticos, conforme relatado por autores como Castells (2003) e Button (2025), que destacam o papel dos espaços digitais descentralizados como facilitadores da ação criminosa.

Além disso, o §4º do art. 171 prevê maiores punições quando a vítima é idosa ou vulnerável, reafirmando a preocupação do ordenamento jurídico com essa população hipervulnerável, como defendem Costa (2025) e Serra et al. (2025). Tal critério reconhece a fragilidade técnica dos idosos, suas limitações cognitivas e a maior probabilidade de manipulação emocional. Contudo, mesmo contando com inovações legislativas, há obstáculos práticos relevantes. A Lei nº 13.964/2019 (Pacote Anticrime) alterou a natureza da ação penal no estelionato, tornando-a pública condicionada à representação. Isso significa que o processo só se inicia mediante manifestação expressa da vítima, o que, na prática, dificulta sobremaneira a persecução penal quando se trata de idosos, muitos dos quais sequer compreendem que foram enganados ou têm receio de denunciar por vergonha, medo de retaliação familiar ou desconhecimento dos procedimentos jurídicos. A dificuldade investigativa é agravada pelo uso de técnicas como: spoofing, servidores estrangeiros (offshore), contas criptografadas, bots automatizados, perfis “laranjas”, deepfakes, e aplicativos de voz e imagem sintetizada.

Estudos do CIDCIBER/Polícia Federal (2024) confirmam que a rastreabilidade desses crimes exige recursos avançados de perícia digital, nem sempre disponíveis na estrutura policial brasileira. A jurisprudência também revela nuances importantes. Embora a legislação seja rigorosa, decisões como o acórdão do TJ-SP (APR: 1505517-22.2018.8.26.0602) demonstram

⁵ A referência ao período pós-2020 relaciona-se ao impacto da pandemia de Covid-19 nas dinâmicas sociais e tecnológicas. O isolamento físico intensificou o uso de meios digitais para atividades cotidianas, serviços bancários, comunicação, compras e interações sociais, ampliando a exposição dos usuários, especialmente idosos, a golpes virtuais. Relatórios de instituições públicas e privadas registraram aumento expressivo das fraudes eletrônicas nesse contexto, o que motivou debates legislativos e contribuiu para a aprovação da Lei nº 14.155/2021, voltada à atualização da resposta penal frente ao novo cenário de criminalidade digital.

que, mesmo diante de vítimas idosas, réus primários têm recebido penas alternativas, gerando debates sobre a efetividade da proteção penal. No STJ, julgados como o REsp 2.077.278/SP (2023) reforçam a responsabilização objetiva das instituições financeiras por falhas que facilitam fraudes, ampliando o diálogo entre esfera penal e civil.

ESTELIONATO CONTRA IDOSO. Prova robusta da autoria e da materialidade delitiva. Réu que obteve vantagem ilícita, no valor de R\$ 8.000,00, em prejuízo da ofendida, pessoa idosa. Prova oral coerente e segura, encontrando respaldo em prova documental. Réu que sequer apresentou justificativa plausível para os seus atos. Condenação mantida. Penas que comportam redução. Básicas fixadas em um sexto acima dos mínimos legais, diante da gravidade do caso concreto. Em seguida, de rigor o reconhecimento da atenuante da menoridade relativa, retornando as penas aos patamares mínimos. Por fim, correto o reconhecimento da causa de aumento do artigo 171, § 4º, do CP (vítima idosa), de modo que as penas são dobradas. Diante da primariedade do réu, possibilidade de substituição da pena corporal por restritivas de direitos e fixação do regime aberto, para o caso de conversão. Recurso parcialmente provido. (TJ-SP - APR: 15055172220188260602 SP 1505517-22.2018.8.26.0602, Relator: Tristão Ribeiro, Data de Julgamento: 11/02/2020, 5ª Câmara de Direito Criminal, Data de Publicação: 11/02/2020).

Assim, o cenário penal brasileiro revela coexistência entre avanços legislativos importantes e limitações práticas que comprometem a resposta estatal diante da complexidade das fraudes digitais.

3.2. Responsabilização civil nas fraudes digitais: análise do dano, do nexo causal, da responsabilidade objetiva e do dever de cuidado reforçado no tratamento de dados pessoais

A responsabilização civil constitui um dos pilares mais relevantes para a proteção das vítimas de estelionato digital, especialmente idosos. Diferentemente da esfera penal, orientada pela punição, o campo civil visa reparar o dano, restabelecer o equilíbrio patrimonial e impor aos agentes envolvidos deveres de vigilância, segurança e prevenção.

O Código Civil, em seu artigo 927, prevê que aquele que causa dano a outrem deve repará-lo. No contexto de fraudes digitais, esse dispositivo dialoga com a responsabilidade das instituições financeiras, das empresas de tecnologia e das entidades que armazenam dados pessoais. Já o Código de Defesa do Consumidor (CDC) reforça essa proteção ao estabelecer a responsabilidade objetiva dos fornecedores de serviços, especialmente os bancos, conforme a Súmula 479 do STJ: “As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias.”

A jurisprudência do STJ tem sido determinante para consolidar essa interpretação. No REsp 2.077.278/SP (2023), a Corte reconheceu a responsabilidade da instituição financeira pelo

vazamento ou tratamento inadequado de dados sensíveis que viabilizaram a fraude. A decisão fundamenta que a falha na prestação do serviço, principalmente quando relacionada à segurança de dados, caracteriza defeito que torna a instituição responsável pelo dano, independentemente de culpa.

Esse entendimento se alinha à crescente preocupação global com a segurança informacional. Segundo Button (2025), idosos são particularmente prejudicados por falhas sistêmicas de segurança digital, pois a exposição de seus dados aumenta a probabilidade de serem vítimas de golpes personalizados, técnica conhecida como fraude por enriquecimento de dados. No âmbito das relações de consumo, os golpes envolvendo empréstimos consignados fraudulentos, boletos falsos e serviços financeiros inexistentes têm crescido exponencialmente, e o STJ tem reiterado que o consumidor idoso deve ser especialmente protegido, devido à sua hipossuficiência técnica. A responsabilidade civil nesses casos inclui tanto danos materiais quanto danos morais, já que o abalo emocional e a perda da sensação de segurança são elementos juridicamente mensuráveis.

Outro aspecto relevante é o dever de cuidado reforçado no tratamento de dados pessoais. Como destaca Costa (2025), entidades que coletam dados de idosos (bancos, clínicas, operadoras, instituições públicas) possuem dever jurídico ampliado para adotar medidas de segurança compatíveis com o risco. Quando há falha, mesmo que o golpe tenha sido praticado por terceiro, incide responsabilidade objetiva. A esfera civil se torna, portanto, fundamental para reparar danos, para estimular boas práticas, impor padrões de segurança e contribuir para a redução do estelionato digital como fenômeno social.

3.3. A responsabilidade administrativa e o papel da LGPD no enfrentamento às fraudes: tratamento de dados pessoais, dever de segurança, incidentes de vazamento e efeitos sobre a população idosa

A Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018) surge como instrumento estratégico para a proteção da pessoa idosa no ambiente digital. Embora não preveja crimes específicos relacionados ao vazamento ou uso indevido de dados, a LGPD cria uma série de obrigações administrativas, impondo deveres de segurança, transparência, finalidade e prevenção aos agentes de tratamento de dados pessoais.

O artigo 46 da LGPD determina que empresas e instituições devem adotar medidas técnicas e administrativas capazes de proteger dados pessoais de acessos não autorizados, destruição, perda, alteração ou qualquer forma de incidente de segurança. Esse dispositivo se

relaciona diretamente com as fraudes que atingem idosos, uma vez que grande parte dos golpes depende do acesso prévio a informações sensíveis.

A Operação Tatu Canastra, mencionada no capítulo anterior, demonstra de maneira categórica, a gravidade desses incidentes. O vazamento de dados de mais de 120 milhões de brasileiros, incluindo endereços, dados bancários, informações previdenciárias e histórico financeiro, ampliou o risco de fraudes personalizadas. Autores como Costa (2025) e Santos & Wojahn (2022) afirmam que esses vazamentos produzem vulnerabilidade estrutural, pois permitem que criminosos utilizem dados reais da vítima para aumentar a credibilidade do golpe.

A LGPD prevê sanções administrativas que podem incluir: advertências, multas de até 2% do faturamento, limitadas a R\$ 50 milhões por infração, publicização da infração, bloqueio e eliminação de dados. Entretanto, a doutrina aponta limitações importantes. A ausência de tipificação penal própria e a falta de integração entre ANPD, Ministério Público e Polícia Civil reduzem a efetividade da proteção. Como observa Lourenção (2024), a LGPD impõe obrigações, mas a responsabilização criminal e civil ainda depende de outros diplomas normativos. Para além disso, idosos são desproporcionalmente afetados por incidentes de vazamento, porque normalmente: não têm domínio sobre ferramentas de proteção digital, não conseguem identificar uso indevido de seus dados, desconhecem canais de denúncia e sofrem maior impacto emocional ao receber mensagens fraudulentas apoiadas em informações reais. Assim, a LGPD, apesar de suas limitações, é peça central no enfrentamento às fraudes digitais, pois estabelece parâmetros mínimos de segurança e prevenção, e orienta a atuação das organizações na proteção dos dados de grupos vulneráveis.

3.4. A proteção jurídica da pessoa idosa no Estatuto do Idoso, CDC e políticas correlatas: dignidade, segurança econômica e combate à exploração financeira

A proteção da pessoa idosa contra fraudes digitais também encontra respaldo significativo no Estatuto do Idoso (Lei nº 10.741/2003) e no Código de Defesa do Consumidor (CDC), diplomas que reforçam a necessidade de tutela diferenciada para esse grupo. O artigo 4º do Estatuto do Idoso estabelece que é dever da família, da comunidade, da sociedade e do Poder Público assegurar ao idoso todos os direitos referentes à vida, saúde, alimentação, educação, cultura, dignidade e respeito. A segurança econômica é elemento implícito e fundamental nesse conjunto, uma vez que golpes patrimoniais afetam diretamente o bem-estar e a dignidade do idoso.

O artigo 39 do Estatuto tipifica práticas abusivas que envolvem exploração financeira, estabelecendo punições para condutas que atentem contra o patrimônio da pessoa idosa. Em fraudes digitais, especialmente as relacionadas a empréstimos consignados, cobranças indevidas, planos de saúde falsos ou serviços fraudulentos, o Estatuto funciona como ferramenta de proteção complementar ao CDC.

O Código de Defesa do Consumidor, por sua vez, assegura mecanismos específicos de proteção contra abusos, incluindo práticas enganosas, cláusulas abusivas, publicidade enganosa e serviços defeituosos. A responsabilidade objetiva dos fornecedores e a teoria do risco do empreendimento tornam-se fundamentais no enfrentamento de golpes digitais, sobretudo quando há falhas de segurança em instituições financeiras ou empresas que coletam dados pessoais.

A jurisprudência do STJ reforça esse entendimento, ao estabelecer que o idoso é hipervulnerável nas relações de consumo, exigindo tratamento mais protetivo. Essa interpretação dialoga com autores como Neri (2019), que apontam que envelhecimento e vulnerabilidade econômica frequentemente se intersectam, produzindo maior risco de exploração. Além disso, políticas públicas como a Política Nacional do Idoso, o Sistema Nacional de Atendimento ao Consumidor (SNDC), e programas de educação financeira reforçam o conjunto de proteções disponíveis, ainda que nem sempre aplicadas de forma eficaz. Dessa maneira, Estatuto do Idoso e o CDC protegem a pessoa idosa de práticas abusivas “em geral” e funcionam como arcabouço jurídico essencial no enfrentamento aos golpes digitais e às formas contemporâneas de exploração econômica.

CONSIDERAÇÕES FINAIS

A análise desenvolvida ao longo deste artigo permitiu compreender o estelionato digital contra idosos como um fenômeno complexo, multidimensional e profundamente enraizado nas dinâmicas tecnológicas, sociais e jurídicas que caracterizam a sociedade informacional contemporânea. Partindo da problematização que orientou a pesquisa, as razões pelas quais o estelionato digital tem se expandido com intensidade entre a população idosa no Brasil e de que modo fatores tecnológicos, estruturais, cognitivos e normativos contribuem para essa vulnerabilidade, bem como as possibilidades de resposta oferecidas pelo ordenamento jurídico, foi possível identificar que a vulnerabilidade do idoso não decorre de um fator isolado, mas da convergência entre fragilidades individuais e falhas sistêmicas.

A investigação demonstrou que a expansão do estelionato digital se estrutura sobre três pilares centrais: (a) a rápida evolução das tecnologias de fraude e das estratégias de engenharia social; (b) a hiperexposição de dados pessoais, agravada por vazamentos massivos que alimentam golpes cada vez mais personalizados; e (c) a condição de hipervulnerabilidade da pessoa idosa, resultante de limitações cognitivas naturais do envelhecimento, baixa alfabetização digital, solidão, confiança excessiva em autoridades aparentes e lacunas na proteção institucional. Desse modo, a pesquisa confirma que a criminalidade digital não pode ser compreendida como escolha individual da vítima, mas como fenômeno que se aproveita de fragilidades estruturais, sendo a pessoa idosa sua principal vítima por razões sociotécnicas amplamente documentadas.

No que se refere aos impactos, verificou-se que as consequências dos golpes ultrapassam o âmbito patrimonial, atingindo dimensões emocionais, relacionais e sociais que comprometem a dignidade, a autonomia e a qualidade de vida do idoso. As perdas financeiras se entrelaçam a sentimentos de culpa, humilhação, insegurança e retração social, o que evidencia que a violência digital possui efeitos duradouros e acumulativos, reforçando a necessidade de atuação preventiva e multidisciplinar.

Em relação à problematização central, a pesquisa responde afirmativamente: os fatores que explicam a crescente incidência do estelionato digital contra idosos derivam da interseção entre avanços tecnológicos apropriados por agentes criminosos, falhas de segurança no tratamento de dados, fragilidades institucionais na proteção dessa população e condições sociais que acentuam a susceptibilidade ao golpe. Da mesma forma, demonstrou que o ordenamento jurídico brasileiro já oferece instrumentos de responsabilização penal, civil e administrativa, embora ainda existam lacunas práticas, especialmente no âmbito investigativo e na efetividade da proteção de dados pessoais.

Quanto aos objetivos propostos, todos foram atendidos: estabeleceu-se base conceitual sólida sobre o estelionato digital e suas modalidades; identificaram-se os golpes mais recorrentes e suas dinâmicas sociais e tecnológicas; analisaram-se os impactos sofridos pelos idosos de forma multidimensional; discutiram-se estratégias de prevenção envolvendo família, Estado, instituições financeiras e políticas públicas; sistematizaram-se mecanismos de responsabilização jurídica, com análise normativa e jurisprudencial pertinente.

Assim, o estudo confirma a necessidade de fortalecer políticas públicas de inclusão e educação digital, aprimorar mecanismos de fiscalização e segurança informacional, intensificar campanhas preventivas e ampliar a atuação do Estado na proteção da pessoa idosa. Também evidencia a urgência de integração entre instituições financeiras, plataformas digitais, órgãos

públicos e a Autoridade Nacional de Proteção de Dados, de modo a criar ecossistema mais seguro e resiliente.

Como perspectivas futuras de pesquisa, duas frentes se mostram especialmente promissoras: investigação sobre o impacto da inteligência artificial generativa, deepfakes e automações maliciosas na potencialização de golpes direcionados a idosos, tema emergente e ainda pouco explorado pela literatura jurídica brasileira; estudos empíricos qualitativos com vítimas idosas, envolvendo entrevistas e análise de narrativas, para compreender com maior profundidade as dimensões subjetivas, emocionais e relacionais da vitimização digital, contribuindo para políticas públicas mais personalizadas e efetivas.

Reafirma-se, por fim, que o enfrentamento ao estelionato digital contra idosos depende de uma abordagem transdisciplinar, solidamente ancorada nos princípios da dignidade, da segurança informacional e da proteção integral, integrando esforços jurídicos, sociais, tecnológicos e educativos. Somente assim será possível promover inclusão digital segura, reduzir a vitimização e garantir ao idoso o pleno exercício de seus direitos na sociedade contemporânea.

REFERÊNCIAS BIBLIOGRÁFICAS

BARBOSA, Mariely Ribeiro. **Crime cibernético e a vulnerabilidade da pessoa idosa na rede mundial de computadores**. Goiânia: PUC Goiás, 2022.

BUTTON, Mark. Preventing fraud and cybercrime in an ageing society. **Journal of Cybersecurity**, 2025. Disponível em: <https://pmc.ncbi.nlm.nih.gov/articles/PMC12182441/>. Acesso em: 18 out. 2025.

CASTELLS, Manuel. **A sociedade em rede**. São Paulo: Paz e Terra, 2003.

CERT.br – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Anuário de Incidentes 2022–2024**. São Paulo: NIC.br, 2024.

CIDCIBER – Polícia Federal. **Relatório Técnico sobre Crimes Cibernéticos contra Idosos**. Brasília, 2024.

COSTA, Bruna Martins. A pessoa idosa enquanto hipervulnerável no contexto das fraudes bancárias e da proteção de dados pessoais. **Revista Avant**, Florianópolis, v. 9, n. 1, p. 177–193, 2025. Disponível em: <https://ojs.sites.ufsc.br/index.php/avant/article/view/8039>. Acesso em: 18 nov. 2025.

FBI – Federal Bureau of Investigation. **Elder Fraud Annual Report 2024**. Washington: U.S. Department of Justice, 2024.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **Relatório 2022–2023**. São Paulo: FBSP, 2023.

LOURENÇÃO, Karina Pataluch. Vazamento de dados: um crime que compromete a segurança e a privacidade dos brasileiros. **LinkedIn**, 2024. Disponível em: <https://pt.linkedin.com/pulse/vazamento-de-dados-um-crime-que-compromete-seguran%C3%A7a-karina-nsmaf>. Acesso em: 18 out. 2025.

MENDONÇA, Rafael A. **Fraudes bancárias e engenharia social: impactos sobre idosos**. Revista Direito Digital, 2023.

MINISTÉRIO DA PREVIDÊNCIA SOCIAL. **Relatório anual de fraudes previdenciárias envolvendo idosos**. Brasília, 2023.

MORAES, João V. **Alfabetização digital na terceira idade**. Revista Envelhecimento Ativo, 2019.

NERI, Anita. **Longevidade e vulnerabilidade social**. Campinas: Papirus, 2019.

RECUERO, Raquel. **Redes sociais na internet**. 3. ed. Porto Alegre: Sulina, 2021.

SAFERNET BRASIL. **Relatório anual de ciber Crimes contra idosos 2023–2024**. São Paulo, 2024.

SAFERNET BRASIL. **Relatório anual sobre golpes contra idosos**. São Paulo, 2024.

SANTOS, Maria L. dos; WOJAHN, Aline S. A vulnerabilidade social de idosos frente a golpes no âmbito digital. **Research, Society and Development**, v. 11, n. 11, 2022.

SERRA, Fábio C. da S. et al. A proteção dos idosos contra crimes cibernéticos no Brasil. **Revista REASE**, 2025.

STJ – Superior Tribunal de Justiça. **Recurso Especial n. 2.077.278/SP**, Rel. Min. Nancy Andrighi, 2023.

TJ-SP – Tribunal de Justiça de São Paulo. **Apelação n. 1505517-22.2018.8.26.0602**, Rel. Tristão Ribeiro, 2020.