Scientia et Ratio
ISSN 2525-8532

OS TRÊS PRINCIPAIS CRIMES CIBERNÉTICOS PRATICADOS CONTRA IDOSOS NO BRASIL ENTRE 2020 E 2022: UMA PESQUISA JURÍDICO-DOCUMENTAL

THE THREE MAIN CYBER CRIMES PERMITTED AGAINST THE ELDERLY IN BRAZIL BETWEEN 2020 AND 2022: A LEGAL-DOCUMENTAL RESEARCH

Artigo submetido em 15 de junho de 2026
Artigo aprovado em 17 de junho de 2026
Artigo publicado em 17 de junho de 2026

Scientia et Ratio
Volume 6 – Número 10 – 2026
ISSN 2525-8532

.

Autor:
Carmen Batista Pereira da Silva
Leiliane dos Santos de Oliveira
Maria Vitória Diniz Silva
Isa Omena Machado de Freitas

.

RESUMO: O presente artigo analisou os três principais crimes cibernéticos praticados contra pessoas idosas no Brasil entre 2020 e 2022, período marcado pela intensificação do uso de

serviços digitais, aplicativos bancários, redes sociais e mensagens instantâneas. A pesquisa adotou abordagem qualitativa, bibliográfica e documental, com base em legislação brasileira, relatórios oficiais, dados estatísticos, jurisprudência do Superior Tribunal de Justiça e artigos científicos recentes sobre vitimização digital, phishing, engenharia social, fraudes eletrônicas e vulnerabilidade de idosos. Os resultados indicaram que as três principais modalidades identificadas foram: o estelionato eletrônico por phishing e páginas falsas; os golpes de engenharia social, especialmente falso familiar e falsa central bancária; e o furto de identidade digital associado à invasão de contas, clonagem de aplicativos e uso indevido de dados. Concluiu-se que essas modalidades concentram os principais riscos cibernéticos enfrentados por pessoas idosas no período analisado, pois exploram a confiança, a baixa familiaridade tecnológica, o uso crescente de serviços digitais e a dificuldade de reação imediata das vítimas. Verificou-se, ainda, que a proteção penal é necessária, mas insuficiente quando dissociada de educação digital, segurança bancária preventiva, produção de dados por faixa etária e políticas públicas de inclusão tecnológica segura.

Palavras-chave: Crimes cibernéticos. Engenharia social. Estelionato eletrônico. Pessoa idosa. Vulnerabilidade digital.

ABSTRACT: This article analyzed the three main cybercrimes committed against older adults in Brazil between 2020 and 2022, a period marked by the increased use of digital services, banking applications, social networks, and instant messaging. The research adopted a qualitative, bibliographic, and documentary approach, based on Brazilian legislation, official reports, statistical data, case law from the Superior Court of Justice, and recent scientific articles on digital victimization, phishing, social engineering, electronic fraud, and the vulnerability of older adults. The results indicated that the three main modalities identified were: electronic fraud through phishing and fake websites; social engineering scams, especially family impersonation and fake banking call centers; and digital identity theft associated with account invasion, messaging app cloning, and misuse of personal data. It was concluded that these modalities concentrate the main cyber risks faced by older adults

during the period analyzed, as they exploit trust, low technological familiarity, the growing use of digital services, and the victims' difficulty in reacting immediately. It was also found that criminal protection is necessary but insufficient when disconnected from digital education, preventive banking security, age-disaggregated data production, and public policies for safe digital inclusion.

Keywords: Cybercrime. Digital vulnerability. Electronic fraud. Older people. Social engineering.

1 INTRODUÇÃO

A digitalização da vida cotidiana modificou a forma pela qual pessoas idosas acessam serviços públicos, benefícios previdenciários, operações bancárias, comunicação familiar e consumo de bens e serviços. No Brasil, os dados da PNAD Contínua TIC indicaram que o percentual de pessoas com 60 anos ou mais que utilizaram internet passou de 24,7% em 2016 para 62,1% em 2022, demonstrando expansão acelerada da inclusão digital desse grupo e, ao mesmo tempo, maior exposição a riscos virtuais (IBGE, 2023).

A pandemia da Covid-19 intensificou essa exposição porque transferiu para ambientes digitais atividades antes resolvidas presencialmente, como pagamentos, atendimentos bancários, compras, comunicação com familiares e acesso a informações de saúde. Estudos sobre criminalidade digital no período apontaram que o isolamento social e o aumento da dependência de tecnologias ampliaram oportunidades para fraudes, ataques de phishing, invasão de contas e manipulação por engenharia social (Buil-Gil et al., 2021).

No caso da população idosa, o problema não decorre da idade como fator isolado, mas da combinação entre maior uso de ferramentas digitais, desigualdade no letramento tecnológico, confiança em contatos aparentemente legítimos, medo de perder autonomia e barreiras para reconhecer a fraude. A literatura nacional aponta que golpes virtuais contra idosos exploram justamente a confiança, a baixa familiaridade tecnológica e a dificuldade de

resposta rápida diante de mensagens aparentemente institucionais ou familiares (Bortot et al., 2024).

A delimitação do tema exige cuidado conceitual, pois nem todas as condutas analisadas se enquadram como crimes cibernéticos próprios em sentido técnico. No contexto jurídico brasileiro, crimes cibernéticos podem ser compreendidos como aqueles praticados por meio da internet, de redes ou de sistemas informáticos. Os crimes cibernéticos próprios são aqueles em que o meio virtual ou informático integra a própria estrutura do tipo penal, enquanto os crimes cibernéticos impróprios correspondem a delitos tradicionais praticados com o auxílio de recursos digitais. Assim, golpes como phishing, falso familiar, falsa central bancária e fraudes por páginas falsas aproximam-se, em regra, de crimes patrimoniais tradicionais potencializados por meios digitais, razão pela qual este artigo adota a expressão "crimes cibernéticos praticados contra pessoas idosas" (ESMPU, 2021).

O problema de pesquisa foi formulado nos seguintes termos: quais foram as três principais modalidades de crimes cibernéticos praticados contra idosos no Brasil entre 2020 e 2022? A pergunta foi construída a partir do recorte temporal do projeto, da intensificação do uso de tecnologias digitais no período pandêmico e da necessidade de compreender quais práticas fraudulentas se tornaram mais recorrentes contra pessoas idosas no ambiente virtual, especialmente diante da expansão de golpes baseados em links falsos, engenharia social, manipulação de confiança e uso indevido de dados pessoais (Bortot et al., 2024).

O objetivo geral consistiu em analisar os três principais crimes cibernéticos praticados contra pessoas idosas no Brasil entre 2020 e 2022. Como objetivos específicos, buscou-se identificar, a partir da literatura científica, da legislação, de dados públicos e de documentos institucionais, as modalidades de crimes cibernéticos mais associadas à vitimização de pessoas idosas no período delimitado; descrever suas principais características jurídicas e operacionais; examinar os fatores que ampliam a vulnerabilidade digital desse grupo; e discutir a resposta legislativa e jurisprudencial aplicável à proteção da pessoa idosa no

ambiente virtual.

A relevância social e jurídica do estudo está no fato de que o envelhecimento populacional e a inclusão digital caminham juntos, exigindo respostas articuladas entre Direito Penal, Direito do Consumidor, proteção de dados, educação digital e políticas públicas. A proteção da pessoa idosa no ambiente virtual não deve limitar sua autonomia, mas criar condições para que ela utilize a tecnologia com segurança, informação adequada, suporte institucional e canais acessíveis de denúncia, especialmente diante da complexidade das fraudes digitais contemporâneas (Serra et al., 2025).

2 METODOLOGIA

A pesquisa adotou abordagem qualitativa, caráter exploratório e natureza bibliográfica e documental, pois examinou o fenômeno a partir de legislação, artigos científicos, relatórios institucionais, dados públicos e jurisprudência. O método dedutivo foi utilizado porque a análise partiu de categorias gerais, como criminalidade cibernética, vulnerabilidade digital e proteção jurídica da pessoa idosa, para interpretar modalidades concretas de golpes virtuais praticados contra esse grupo no período de 2020 a 2022 (Gil, 2022).

A etapa bibliográfica considerou estudos nacionais e internacionais sobre crimes cibernéticos, phishing, engenharia social, fraudes eletrônicas, vitimização de pessoas idosas, alfabetização midiática e prevenção de golpes. Foram priorizados artigos recentes, publicados sobretudo entre 2020 e 2025, a fim de garantir aderência ao contexto pós-pandemia e às transformações tecnológicas observadas no período delimitado, sem perder de vista a necessidade de selecionar fontes diretamente relacionadas ao problema de pesquisa (Gil, 2022).

A etapa documental abrangeu o exame da legislação brasileira relacionada à proteção da pessoa idosa, à tutela penal dos crimes informáticos, à proteção de dados pessoais e ao uso da internet no Brasil, com destaque para a Lei nº 14.155/2021, que tornou mais graves os

crimes de invasão de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet (Brasil, 2021).

Também foram utilizados dados públicos e relatórios institucionais para contextualizar a expansão do acesso à internet e a reorganização das fraudes patrimoniais no ambiente digital, especialmente no período posterior à intensificação do uso de serviços on-line pela população brasileira (Fórum Brasileiro de Segurança Pública, 2023).

A análise jurisprudencial considerou o entendimento consolidado sobre a responsabilidade das instituições financeiras em situações de fraudes praticadas por terceiros no âmbito de operações bancárias, especialmente quando o dano decorre de risco inerente à própria atividade financeira. Essa opção se justifica porque parte dos golpes digitais contra idosos envolve contas bancárias, aplicativos de pagamento, empréstimos, Pix, boletos e movimentações financeiras atípicas, exigindo a análise do dever de segurança, prevenção e identificação de operações incompatíveis com o perfil do consumidor (Portes; Markus, 2025).

A delimitação temporal do estudo correspondeu ao período de março de 2020 a dezembro de 2022, marco associado à intensificação do uso de serviços digitais durante a pandemia da Covid-19. Embora o recorte empírico tenha se limitado a esse intervalo, foram utilizados estudos posteriores apenas como suporte interpretativo e atualização teórica, sem alteração do período analisado, uma vez que parte da literatura e dos relatórios nacionais sobre fraudes digitais consolidou suas análises após a observação dos efeitos sociais e tecnológicos do período pandêmico (Fórum Brasileiro de Segurança Pública, 2023). A principal limitação metodológica identificada foi a ausência de uma base pública nacional padronizada que apresentasse, por faixa etária, um ranking completo e detalhado dos crimes cibernéticos praticados contra idosos no Brasil entre 2020 e 2022. Por essa razão, a pesquisa foi direcionada uma Revisão Bibliográfica e Documental Integrativa.

Diante da ausência de uma base estatística pública nacional unificada que apresentasse, por

faixa etária, um ranking completo dos crimes cibernéticos praticados contra pessoas idosas no Brasil entre 2020 e 2022, a seleção das três modalidades analisadas não foi realizada por critério quantitativo absoluto, mas por amostragem intencional e triangulação qualitativa entre fontes bibliográficas, documentais, legislativas e jurisprudenciais. Para os fins deste estudo, consideraram-se "principais" as modalidades que apresentaram maior convergência entre: a recorrência temática na literatura científica nacional sobre golpes virtuais contra idosos; a pertinência jurídico-penal em relação à Lei nº 14.155/2021; a presença em documentos institucionais sobre fraudes digitais e segurança na internet; e a relação com discussões jurisprudenciais sobre responsabilidade bancária, proteção do consumidor e fortuito interno.

O processo de seleção ocorreu em três etapas. Na primeira, realizou-se o mapeamento inicial de práticas digitais associadas à vitimização patrimonial de pessoas idosas, a partir de estudos nacionais, relatórios institucionais, legislação e documentos de orientação sobre segurança digital. Nesse levantamento, foram identificadas práticas como phishing, páginas falsas, falso empréstimo consignado, golpe do falso familiar, falsa central bancária, clonagem de aplicativo de mensagens, invasão de contas, uso indevido de dados pessoais, golpes afetivos e outras fraudes praticadas por meios digitais.

Na segunda etapa, aplicou-se um filtro de pertinência jurídica e documental. Foram priorizadas as modalidades que apresentavam relação mais direta com os tipos penais de estelionato eletrônico, furto mediante fraude, invasão de dispositivo informático ou uso indevido de dados pessoais, especialmente após as alterações promovidas pela Lei nº 14.155/2021. Também foram considerados os golpes que apareciam de forma reiterada na literatura nacional sobre pessoas idosas e fraudes digitais, em documentos de orientação de segurança na internet e em debates jurisprudenciais envolvendo instituições financeiras, aplicativos bancários, transações eletrônicas e responsabilidade do fornecedor de serviços digitais.

Na terceira etapa, foram excluídas as modalidades que, embora relevantes no campo da criminalidade digital, não apresentaram aderência suficiente ao recorte do artigo. Assim, práticas como ransomware, golpes afetivos, fraudes genéricas de comércio eletrônico e outras modalidades específicas foram afastadas quando não se mostraram diretamente vinculadas, no material analisado, à vitimização recorrente de pessoas idosas no Brasil entre 2020 e 2022, ou quando não apresentaram conexão mais evidente com a resposta penal e jurisprudencial examinada no estudo.

Com base nesse procedimento, foram selecionadas três categorias analíticas: estelionato eletrônico por phishing, links e páginas falsas; golpes de engenharia social, especialmente falso familiar e falsa central bancária; e furto de identidade digital associado à invasão de contas, clonagem de aplicativos e uso indevido de dados pessoais. Essas categorias não foram tratadas como ranking estatístico nacional absoluto, mas como eixos de maior convergência qualitativa entre as fontes examinadas, pois reúnem pertinência penal, relevância documental, recorrência na literatura sobre golpes contra idosos e conexão com a vulnerabilidade digital da pessoa idosa. Reconhece-se, portanto, como limitação metodológica, que a classificação decorre de análise bibliográfica e documental, e não de base nacional padronizada de ocorrências criminais por faixa etária, inexistente para o recorte específico adotado.

3 PROTEÇÃO JURÍDICA DA PESSOA IDOSA NO AMBIENTE DIGITAL

A proteção da pessoa idosa no Brasil possui fundamento constitucional, pois a Constituição Federal de 1988 estabelece a dignidade da pessoa humana como fundamento da República e atribui à família, à sociedade e ao Estado o dever de amparar as pessoas idosas, assegurando sua participação na comunidade e a defesa de sua dignidade e bem-estar (Brasil, 1988).

No ambiente digital, esse dever de proteção assume nova dimensão, uma vez que o

exercício da cidadania contemporânea depende cada vez mais do acesso seguro a serviços públicos, informações, plataformas financeiras, canais de comunicação e recursos tecnológicos. Assim, a inclusão digital da pessoa idosa deve ser compreendida como instrumento de autonomia, participação social e proteção contra novas formas de exclusão e vulnerabilidade (Menezes; Bora; Alves, 2023).

O Estatuto da Pessoa Idosa, instituído pela Lei nº 10.741/2003, assegura direitos à pessoa com idade igual ou superior a 60 anos e prevê proteção contra negligência, discriminação, violência, crueldade e opressão. Essa proteção legal reforça o dever do Estado, da sociedade e da família de resguardar a dignidade, a segurança e o bem-estar da pessoa idosa em diferentes contextos de vulnerabilidade (Brasil, 2003).

Embora o Estatuto tenha sido elaborado antes da consolidação de muitas práticas digitais atuais, seus princípios permitem interpretar golpes virtuais, fraudes bancárias e violência patrimonial on-line como formas contemporâneas de violação da dignidade e da segurança da pessoa idosa. Nesse sentido, a proteção jurídica precisa acompanhar as novas modalidades de exposição e risco produzidas pelo uso crescente de tecnologias digitais (Serra et al., 2025).

A vulnerabilidade digital não deve ser confundida com incapacidade civil ou ausência de autonomia. A pessoa idosa pode ser plenamente capaz e, ainda assim, encontrar-se em situação de risco diante de interfaces pouco acessíveis, linguagem técnica, mensagens fraudulentas convincentes, baixa familiaridade com mecanismos de segurança e pressão psicológica criada pelos golpistas. Desse modo, a vulnerabilidade deve ser compreendida como fenômeno contextual e relacional, associado às desigualdades tecnológicas, à assimetria informacional e às estratégias de manipulação utilizadas nas fraudes on-line (Shang et al., 2022).

O crescimento do uso da internet por pessoas idosas amplia oportunidades de participação

social, acesso a serviços e autonomia, mas também exige políticas de alfabetização digital e educação midiática. Experiências formativas voltadas a esse público demonstram que estratégias pedagógicas adaptadas, linguagem acessível, exemplos práticos e acompanhamento adequado podem contribuir para o reconhecimento de conteúdos enganosos, mensagens suspeitas e pedidos financeiros fraudulentos (Figueiredo; Antonioli; Gil, 2023).

A Lei Geral de Proteção de Dados Pessoais relaciona-se diretamente ao tema porque muitos golpes contra pessoas idosas envolvem coleta indevida, vazamento ou uso abusivo de dados pessoais, como CPF, telefone, endereço, informações bancárias, dados previdenciários e histórico de consumo. Em golpes de falsa central, falso boleto ou phishing, a utilização de dados verdadeiros aumenta a aparência de legitimidade da abordagem criminosa e dificulta a identificação imediata da fraude pela vítima (Brasil, 2018).

O Marco Civil da Internet também oferece suporte à análise ao estabelecer princípios, garantias, direitos e deveres para o uso da internet no Brasil, incluindo a proteção da privacidade, dos dados pessoais e dos registros de conexão. Embora não tenha natureza penal, sua função normativa é relevante para a definição de responsabilidades, preservação de provas digitais e estruturação da cooperação entre usuários, provedores, plataformas e autoridades (Brasil, 2014).

4 CRIMINALIDADE CIBERNÉTICA E DELITOS CONTRA IDOSOS

A criminalidade cibernética compreende condutas em que computadores, redes, sistemas, dispositivos móveis e dados digitais aparecem como meio, instrumento, ambiente ou alvo da ação criminosa. Nesse campo, distinguem-se os crimes dependentes de tecnologia, que somente podem ser praticados mediante o uso de sistemas, redes ou dispositivos informáticos, dos crimes facilitados por tecnologia, nos quais delitos tradicionais, como furto, estelionato ou extorsão, são executados ou potencializados por meios digitais (Escola

Superior do Ministério Público da União, 2021).

No contexto dos golpes contra pessoas idosas, grande parte das condutas analisadas se enquadra como criminalidade patrimonial facilitada por meios digitais, e não necessariamente como crime cibernético próprio em sentido estrito. Práticas como phishing, falso familiar, falsa central bancária e falso atendimento de órgãos públicos costumam operar por meio de fraude, induzimento em erro e manipulação da confiança da vítima, ainda que também possam envolver invasão de contas, clonagem de aplicativos ou uso indevido de identidade digital (Bortot et al., 2024).

A pandemia alterou o campo de oportunidades criminosas, deslocando parte das práticas patrimoniais para ambientes digitais. Durante os períodos de maior restrição de circulação, houve intensificação do uso de serviços on-line, o que ampliou a exposição de usuários a fraudes virtuais, invasões de contas e outras formas de criminalidade cibernética associadas à mudança repentina das rotinas sociais e econômicas (Buil-Gil et al., 2021).

Além disso, os golpes digitais praticados no contexto pandêmico exploraram medo, urgência, desinformação e dependência tecnológica, elementos que favoreceram ataques de phishing e estratégias de engenharia social. Esse cenário tornou pessoas idosas mais expostas a mensagens fraudulentas relacionadas a bancos, saúde, benefícios, compras on-line e contatos aparentemente legítimos (Bortot et al., 2024).

No Brasil, o Fórum Brasileiro de Segurança Pública indicou crescimento expressivo dos estelionatos no período recente e chamou atenção para a reorganização dos crimes patrimoniais, marcada pela redução relativa de algumas modalidades presenciais e pela expansão das fraudes eletrônicas. Esse cenário evidencia que a criminalidade patrimonial passou a incorporar com maior intensidade o ambiente digital, especialmente em golpes praticados por meio de aplicativos, plataformas bancárias, mensagens e canais virtuais de atendimento (Fórum Brasileiro de Segurança Pública, 2023).

Nesse contexto, a Lei nº 14.155/2021 agravou as penas aplicáveis aos crimes de invasão de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet, reconhecendo a maior gravidade das condutas praticadas mediante uso de redes sociais, contatos telefônicos, correio eletrônico fraudulento ou outros meios digitais capazes de induzir a vítima em erro (Brasil, 2021).

Esse crescimento, contudo, não permite afirmar, de forma estatística absoluta, que as pessoas idosas foram as principais vítimas de todos os crimes digitais, uma vez que ainda há limitação de dados nacionais sistematizados por faixa etária. Ainda assim, a expansão do acesso de idosos à internet e o aumento das fraudes eletrônicas indicam um campo de risco que justifica investigação jurídica específica sobre a vitimização digital desse grupo (IBGE, 2023).

5 AS TRÊS PRINCIPAIS MODALIDADES IDENTIFICADAS

5.1 Estelionato eletrônico por phishing, links e páginas falsas

A primeira modalidade identificada é o estelionato eletrônico por phishing, links maliciosos e páginas falsas. O phishing consiste em induzir a vítima a acreditar que está diante de comunicação legítima, levando-a a informar senhas, códigos, dados pessoais, dados bancários ou a acessar páginas fraudulentas que simulam bancos, órgãos públicos, lojas virtuais, programas sociais ou serviços previdenciários (CERT.br, 2025).

No plano jurídico, a Lei nº 14.155/2021 incluiu no art. 171, § 2º-A, do Código Penal a fraude eletrônica, com pena mais severa quando a fraude é cometida com uso de informações fornecidas pela vítima ou por terceiro induzido a erro, por meio de redes sociais, contatos telefônicos, correio eletrônico fraudulento ou outro meio fraudulento análogo. Essa previsão dialoga diretamente com a lógica do phishing, pois o êxito do golpe depende da participação enganada da própria vítima (Brasil, 2021).

No recorte envolvendo idosos, o phishing ganhou maior potencial lesivo com a digitalização de serviços bancários e previdenciários. Mensagens falsas de atualização cadastral, bloqueio de benefício, confirmação de Pix, consulta de CPF, falso boleto ou falsa compra aproveitam rotinas digitais recentes e podem ser mais convincentes quando contêm dados reais da vítima ou aparência visual semelhante à de instituições legítimas (Azevedo; Vidigal; Sales, 2025).

Azevedo, Vidigal e Sales (2025) destacam que a prevenção de golpes virtuais contra idosos exige linguagem acessível, exemplos concretos e orientação prática. Por isso, campanhas baseadas apenas em frases genéricas, como “não clique em links”, tendem a ser insuficientes quando não explicam como os golpes são construídos e como a vítima pode confirmar a autenticidade de uma mensagem.

5.2 Golpes de engenharia social: falso familiar e falsa central

A segunda modalidade corresponde aos golpes de engenharia social, especialmente falso familiar, falso parente, falso funcionário de banco e falsa central de atendimento. Nesses casos, o elemento central não é necessariamente a sofisticação técnica do ataque, mas a manipulação psicológica que leva a vítima a agir rapidamente, acreditar no interlocutor, fornecer informações sensíveis ou realizar transferências financeiras sob pressão emocional ou falsa sensação de urgência (Bortot et al., 2024).

No golpe do falso familiar, o criminoso se passa por filho, neto, sobrinho ou pessoa próxima, geralmente por aplicativo de mensagens, informa ter trocado de número e solicita pagamento urgente. A prática explora vínculos afetivos, senso de responsabilidade familiar e medo de que alguém próximo esteja em dificuldade, razão pela qual se mostra especialmente relevante quando direcionada a pessoas idosas que mantêm comunicação cotidiana com familiares pelo celular (Bortot et al., 2024).

Na falsa central bancária, o golpista simula atendimento institucional, afirma que houve

tentativa de fraude, pede confirmação de dados, orienta a instalação de aplicativo, solicita código enviado por SMS ou induz a vítima a transferir valores para uma suposta “conta segura”. A fraude se torna mais convincente quando há conhecimento prévio de informações bancárias ou pessoais da vítima, o que aproxima a conduta de problemas relacionados à proteção de dados, à segurança informacional e ao dever de prevenção das instituições financeiras (Portes; Markus, 2025).

Nos golpes de falsa identidade, os criminosos constroem uma encenação de autoridade, proximidade ou urgência para reduzir o tempo de reflexão da vítima. A engenharia social também se adapta ao perfil do alvo: em pessoas idosas, tende a explorar confiança em instituições, medo de perder benefício ou conta bancária, desejo de ajudar familiares e receio de demonstrar desconhecimento tecnológico (Azevedo; Vidigal; Sales, 2025).

A prevenção dessa modalidade exige estratégias diferentes daquelas voltadas apenas à proteção de senhas. Além de autenticação em duas etapas, bloqueio de contatos suspeitos e confirmação por outro canal, é necessário ensinar a pessoa idosa a reconhecer sinais narrativos do golpe, como pressa, segredo, ameaça, promessa de solução imediata, pedido de código, troca repentina de número e recusa em fazer chamada de vídeo ou ligação por canal habitual (Serra et al., 2025).

5.3 Furto de identidade digital, invasão de contas e uso indevido de dados

A terceira modalidade é o furto de identidade digital, associado à invasão de dispositivos, tomada de contas, clonagem de aplicativos de mensagens e uso indevido de dados pessoais. Nessa categoria, o criminoso deixa de apenas enganar a vítima diretamente e passa a utilizar sua identidade digital para acessar serviços, abordar terceiros, solicitar dinheiro, movimentar contas ou ampliar o alcance da fraude, explorando a confiança construída em torno do nome, da imagem e dos contatos da pessoa idosa (Bortot et al., 2024).

No plano jurídico, o art. 154-A do Código Penal tipifica a invasão de dispositivo informático de

uso alheio, conectado ou não à rede de computadores, com a finalidade de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário. Embora nem toda clonagem de aplicativo se enquadre automaticamente nesse tipo penal, a norma é relevante para compreender a proteção jurídica de dados, contas e dispositivos no ambiente digital (Brasil, 1940).

Contra pessoas idosas, o furto de identidade digital assume gravidade específica porque pode comprometer redes de confiança familiar e comunitária. Quando uma conta de mensagem é tomada, o criminoso fala em nome da vítima e aciona contatos que confiam nela; quando dados bancários são apropriados, a fraude pode produzir empréstimos, compras, transferências e boletos falsos que geram prejuízos prolongados e dificultam a recomposição patrimonial e emocional da vítima (Serra et al., 2025).

Contra pessoas idosas, o furto de identidade digital assume gravidade específica porque pode comprometer redes de confiança familiar e comunitária. Quando uma conta de mensagem é tomada, o criminoso fala em nome da vítima e aciona contatos que confiam nela; quando dados bancários são apropriados, a fraude pode produzir empréstimos, compras, transferências e boletos falsos, ampliando os riscos patrimoniais e dificultando a interrupção rápida do golpe (Serra et al., 2025).

As três modalidades analisadas não funcionam de modo isolado. Um golpe pode começar com phishing para captura de dados, avançar para engenharia social por telefone ou mensagem e terminar com tomada de conta, empréstimo, Pix ou uso indevido de identidade digital. Essa interligação justifica uma abordagem jurídica e preventiva integrada, capaz de considerar a cadeia completa da fraude e não apenas o ato final de transferência financeira (Button et al., 2024).

6 MATRIZ DE RESULTADOS DA ANÁLISE DOCUMENTAL

Com base na análise legislativa, bibliográfica, documental e jurisprudencial, o quadro a

seguir sintetiza as três modalidades identificadas como mais relevantes para o recorte do estudo. A síntese não pretende afirmar um ranking estatístico nacional absoluto, mas organizar, em matriz qualitativa, os padrões de golpes cibernéticos contra pessoas idosas que apresentaram maior pertinência jurídica e maior recorrência temática nos documentos e estudos analisados (Bortot et al., 2024).

Quadro 1 – Síntese das modalidades analisadas

Modalidade	Descrição operacional	Base jurídica aproximada	Fatores de risco para idosos	Fontes principais
Estelionato eletrônico por phishing	Links, mensagens, e-mails, páginas falsas e formulários fraudulentos para captura de dados, senhas, códigos ou pagamentos.	Art. 171, § 2º-A, do Código Penal, com redação da Lei nº 14.155/2021.	Baixo letramento digital, aparência institucional da mensagem, urgência, medo de bloqueio de benefício ou conta.	Brasil (2021); CERT.br (2025); Bortot et al. (2024).
Golpes de engenharia social	Falso familiar, falso funcionário de banco, falsa central, falso atendente do INSS e pedidos urgentes de dinheiro ou códigos.	Estelionato, fraude eletrônica e eventuais crimes conexos, conforme a forma de execução.	Confiança em vínculos familiares e instituições, pressão emocional, dificuldade de verificar rapidamente a identidade do interlocutor.	Bortot et al. (2024); Azevedo, Vidigal e Sales (2025).
Furto de identidade digital e invasão de contas	Tomada de contas de mensagens, uso indevido de dados, clonagem de aplicativos, acesso não autorizado e uso da identidade da vítima.	Art. 154-A do Código Penal, Lei nº 12.737/2012, Lei nº 14.155/2021, LGPD e normas de consumo.	Dependência do celular, reutilização de senhas, exposição de dados, dificuldade de recuperar contas e denunciar rapidamente.	Brasil (2012; 2018; 2021); Bortot et al. (2024); Portes; Markus (2025).

Fonte: elaboração própria, com base em CERT.br (2025), Bortot et al. (2024) e Azevedo, Vidigal e Sales (2025).

O quadro demonstra que os crimes cibernéticos contra pessoas idosas formam um ecossistema de fraude digital. A vítima pode ser atraída por phishing, convencida por engenharia social e, posteriormente, ter seus dados, contas ou identidade digital apropriados para novos golpes. Essa dinâmica reforça a necessidade de prevenção em múltiplas camadas, envolvendo educação digital, segurança bancária, proteção de dados pessoais, canais acessíveis de denúncia, suporte pós-vitimação e responsabilização adequada dos agentes envolvidos (Button et al., 2024).

7 RESPONSABILIDADE CIVIL, JURISPRUDÊNCIA E PROTEÇÃO DO CONSUMIDOR IDOSO

A responsabilização jurídica dos crimes cibernéticos contra pessoas idosas não se limita ao campo penal. Em muitos casos, a fraude ocorre em ambiente de consumo, especialmente quando envolve bancos, financeiras, plataformas de pagamento, aplicativos e prestadores de serviços digitais, de modo que a análise deve considerar também o dever de segurança, informação adequada e prevenção de danos nas relações entre fornecedores e consumidores (Brasil, 1990).

O Superior Tribunal de Justiça consolidou, pela Súmula 479, o entendimento de que as instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias. Esse entendimento se fundamenta na teoria do risco do empreendimento e no dever de segurança inerente à atividade financeira (Brasil, STJ, 2012).

A aplicação da responsabilidade objetiva em golpes digitais depende da análise do caso concreto. Quando há transações incompatíveis com o perfil do cliente, falha de autenticação, ausência de bloqueio preventivo ou insuficiência de mecanismos de segurança, reforça-se a

responsabilidade da instituição financeira; por outro lado, quando demonstrada a adoção de medidas adequadas e a ocorrência de conduta externa imprevisível, pode haver discussão sobre culpa exclusiva da vítima ou de terceiro (Portes; Markus, 2025).

A condição de pessoa idosa não gera indenização automática, mas deve ser considerada na avaliação da vulnerabilidade, da linguagem informacional, do dever de cuidado e da expectativa legítima de segurança. Em relações de consumo digitais, pessoas idosas podem se encontrar em situação de hipervulnerabilidade diante de operações complexas, contratos eletrônicos, aplicativos bancários e mensagens fraudulentas que simulam canais oficiais (Volpato; Pegoraro Junior, 2024).

A jurisprudência deve evitar raciocínio que transfira integralmente à vítima idosa a responsabilidade pelo golpe. Em fraudes digitais, especialmente nas bancárias, a análise jurídica precisa considerar que a engenharia social é planejada para induzir erro, explorar confiança, medo, pressa e assimetria técnica. Por isso, a conduta da vítima deve ser avaliada em conjunto com o grau de previsibilidade do risco, a compatibilidade das transações com o perfil do consumidor e o dever institucional de reduzir danos evitáveis no ambiente financeiro digital (Portes; Markus, 2025).

A proteção jurídica mais adequada combina repressão ao agente criminoso, reparação civil quando houver falha de serviço, dever de cooperação das plataformas, educação digital e canais de atendimento humanizados. Modelos eficazes de prevenção contra fraudes envolvendo pessoas idosas devem ser holísticos, articulando tecnologia, políticas públicas, instituições financeiras, família, comunidade e suporte pós-vitimação, de modo a proteger a autonomia da pessoa idosa sem restringir sua participação no ambiente digital (Button et al., 2024).

8 DISCUSSÃO

A análise dos resultados demonstra que a vulnerabilidade digital da pessoa idosa não decorre

apenas da idade, mas da combinação entre inclusão digital acelerada, desigualdade no letramento tecnológico, confiança em comunicações aparentemente legítimas e dificuldade de verificação imediata das informações recebidas. No Brasil, o crescimento do acesso à internet por pessoas com 60 anos ou mais ampliou a participação desse grupo em serviços bancários, redes sociais, aplicativos de mensagens, compras on-line e atendimentos digitais. Contudo, essa inserção ocorreu de forma desigual, sem que todos os usuários idosos tivessem recebido orientação suficiente sobre segurança digital, reconhecimento de golpes e proteção de dados pessoais (IBGE, 2023).

Esse cenário ajuda a explicar a pertinência das três modalidades selecionadas neste estudo. O estelionato eletrônico por phishing, links e páginas falsas explora, sobretudo, a aparência de legitimidade de mensagens, sites e comunicações que simulam bancos, órgãos públicos, lojas virtuais ou serviços previdenciários. Para a pessoa idosa, a dificuldade não está apenas em usar a tecnologia, mas em distinguir uma comunicação verdadeira de uma fraudulenta, especialmente quando a mensagem apresenta linguagem institucional, logotipos, dados pessoais ou ameaça de bloqueio de conta, benefício ou serviço (CERT.br, 2025).

Nos golpes de engenharia social, como falso familiar e falsa central bancária, a vulnerabilidade se manifesta pela manipulação da confiança. O criminoso não depende necessariamente de técnica sofisticada, mas de uma narrativa convincente, construída com urgência, medo, autoridade ou vínculo afetivo. Assim, quando o golpista se apresenta como parente, funcionário de banco ou atendente de instituição conhecida, a vítima pode ser induzida a realizar transferências, fornecer códigos, confirmar dados ou seguir instruções sem tempo adequado para checagem (Azevedo; Vidigal; Sales, 2025).

O furto de identidade digital, a invasão de contas e o uso indevido de dados pessoais evidenciam outro fator de vulnerabilidade: a exposição de informações pessoais no ambiente digital. Dados como CPF, telefone, endereço, informações bancárias, contatos familiares e histórico de consumo podem ser utilizados para tornar o golpe mais convincente e ampliar

sua capacidade de engano. Nesse ponto, a proteção da pessoa idosa também depende do controle sobre a coleta, o armazenamento e o uso de seus dados por instituições, empresas, plataformas e terceiros (Brasil, 2018).

A legislação penal brasileira reconheceu a gravidade desse cenário com a Lei nº 14.155/2021, que tornou mais graves os crimes de invasão de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet. A norma é importante porque aproxima a resposta penal das novas formas de fraude digital, mas não resolve sozinha o problema, já que os fatores de vulnerabilidade também envolvem educação digital, segurança bancária, acessibilidade das plataformas e prevenção institucional (Brasil, 2021).

Nas relações de consumo, especialmente bancárias, a vulnerabilidade da pessoa idosa exige atenção ao dever de segurança dos fornecedores. Bancos e instituições financeiras devem adotar mecanismos capazes de reduzir riscos previsíveis, identificar movimentações incompatíveis com o perfil do cliente e oferecer canais de atendimento claros e acessíveis. Em golpes digitais, não se deve transferir automaticamente à vítima idosa toda a responsabilidade pela fraude, sobretudo quando houver falha de segurança ou ausência de bloqueio preventivo (Portes; Markus, 2025).

Dessa forma, a discussão confirma que os três crimes analisados possuem relação direta com fatores de vulnerabilidade digital da população idosa: o phishing explora a dificuldade de identificar comunicações falsas; a engenharia social explora vínculos de confiança e urgência; e o furto de identidade digital explora a exposição e o uso indevido de dados pessoais. Por isso, o enfrentamento dos crimes cibernéticos contra idosos exige medidas integradas de alfabetização digital, proteção de dados, segurança bancária preventiva, orientação familiar, campanhas educativas acessíveis e atuação coordenada entre Estado, instituições financeiras e plataformas digitais (Serra et al., 2025).

9 CONSIDERAÇÕES FINAIS

O artigo analisou os três principais crimes cibernéticos praticados contra pessoas idosas no Brasil entre 2020 e 2022, a partir do contexto de expansão do uso da internet, intensificação das atividades digitais durante a pandemia e aumento das fraudes patrimoniais mediadas por tecnologia. A pesquisa demonstrou que o fenômeno deve ser interpretado de modo jurídico, social e tecnológico, pois envolve legislação penal, proteção de dados, direito do consumidor, envelhecimento e inclusão digital. (IBGE, 2023; Buil-Gil et al., 2021; Serra et al., 2025).

A primeira modalidade identificada foi o estelionato eletrônico por phishing, links falsos e páginas fraudulentas, em que a vítima é induzida a fornecer dados, senhas, códigos ou valores. Essa modalidade ganhou resposta legislativa mais severa com a Lei nº 14.155/2021, que inseriu a fraude eletrônica no Código Penal e reconheceu a gravidade do uso de meios digitais na prática do estelionato. (Brasil, 2021; Cert.br, 2025; Naidoo, 2020).

A segunda modalidade foi a engenharia social, especialmente falso familiar e falsa central bancária, marcada pela manipulação de vínculos de confiança, urgência, medo e autoridade institucional. A análise mostrou que esse tipo de golpe exige medidas preventivas específicas, pois não se combate apenas com tecnologia, mas também com educação digital, confirmação por canais independentes e fortalecimento da autonomia decisória da pessoa idosa. (Shapiro, 2025; Azevedo; Vidigal; Sales, 2025; Button et al., 2024).

A terceira modalidade foi o furto de identidade digital, associado à invasão de contas, clonagem de aplicativos de mensagens e uso indevido de dados pessoais. Essa prática é especialmente grave porque compromete não apenas o patrimônio da vítima, mas também sua rede de relações, sua imagem, sua confiança e sua capacidade de circular com segurança no ambiente digital. (Brasil, 2012; Havers et al., 2024; Bortot et al., 2024).

No campo jurisprudencial, verificou-se que a Súmula 479 do Superior Tribunal de Justiça fornece base relevante para responsabilizar instituições financeiras quando a fraude digital

decorrer de fortuito interno, falha de segurança, ausência de monitoramento ou transações incompatíveis com o perfil do cliente. Essa compreensão é reforçada por Portes e Markus (2025), ao discutirem a atualização do fortuito interno bancário diante das fraudes digitais e do dever de vigilância tecnológica das instituições financeiras. Ao mesmo tempo, a responsabilização deve ser analisada caso a caso, evitando tanto a impunidade institucional quanto a presunção automática de culpa da vítima idosa (Brasil, STJ, 2012; Portes; Markus, 2025).

Conclui-se que o enfrentamento dos crimes cibernéticos contra idosos exige políticas públicas de alfabetização digital, produção de estatísticas específicas por faixa etária, melhoria dos canais de denúncia, atuação preventiva de bancos e plataformas, proteção rigorosa de dados pessoais e campanhas educativas baseadas em situações reais. Proteger a pessoa idosa no ambiente digital significa garantir dignidade, autonomia e participação social com segurança, e não afastá-la dos recursos tecnológicos que já fazem parte da vida contemporânea. (Button et al., 2024; Figueiredo; Antonioli; Gil, 2023; Azevedo; Vidigal; Sales, 2025).

REFERÊNCIAS

AZEVEDO, Sandra Ribeiro de; VIDIGAL, Juliana Gonçalves; SALES, Diego da Silva. Fake news e golpes virtuais em idosos: desafios e intervenções educativas. *ARACÊ*, [S. l.], v. 7, n. 8, p. e7622, 2025. DOI: 10.56238/arev7n8-250. Disponível em: https://periodicos.newsciencepubl.com/arace/article/view/7622. Acesso em: 21 maio 2026.

BORTOT, Erine Natalie; FRANZ, Lisa Marie; GUERRA, Marcus Vinícius; GODOY, Wilson Itamar. Teias de engano: uma análise dos riscos e estratégias de prevenção aos golpes cibernéticos praticados contra pessoas idosas na era digital. *Contribuciones a las Ciencias Sociales*, [S. l.], v. 17, n. 13, 2024. Disponível em: https://ojs.revistacontribuciones.com/ojs/index.php/clcs/article/view/13534. Acesso em: 21

maio 2026.

BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 21 maio 2026.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. Brasília, DF: Presidência da República, 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 21 maio 2026.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Código de Defesa do Consumidor. Brasília, DF: Presidência da República, 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 21 maio 2026.

BRASIL. Lei nº 10.741, de 1º de outubro de 2003. Dispõe sobre o Estatuto da Pessoa Idosa e dá outras providências. Brasília, DF: Presidência da República, 2003. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2003/l10.741.htm. Acesso em: 21 maio 2026.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos. Brasília, DF: Presidência da República, 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 21 maio 2026.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 21 maio 2026.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais.

Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 21 maio 2026.

BRASIL. Lei nº 14.155, de 27 de maio de 2021. Altera o 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. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm. Acesso em: 21 maio 2026.

BRASIL. Superior Tribunal de Justiça. Súmula nº 479. As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias. Brasília, DF: STJ, 2012. Disponível em: https://arquivocidadao.stj.jus.br/index.php/sumula-479-2. Acesso em: 21 maio 2026.

BUIL-GIL, David; MIRÓ-LLINARES, Fernando; MONEVA, Asier; KEMP, Steven; DÍAZ-CASTAÑO, Nacho. Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. *European Societies*, v. 23, supl. 1, p. S47-S59, 2021. DOI: https://doi.org/10.1080/14616696.2020.1804973. Disponível em: https://www.tandfonline.com/doi/abs/10.1080/14616696.2020.1804973. Acesso em: 21 maio 2026.

BUTTON, M ark; KARAGIANNOPOULOS, Vasileios; LEE, Julak; SUH, Joon Bae; JUNG, Jeyong. Preventing fraud victimisation against older adults: towards a holistic model for protection. *International Journal of Law, Crime and Justice*, v. 77, art. 100672, 2024. DOI: 10.1016/j.ijlcj.2024.100672. Disponível em: https://www.sciencedirect.com/science/article/pii/S1756061624000247. Acesso em: 21 maio 2026.

CERT.BR. Cartilha de Segurança para Internet. São Paulo: Comitê Gestor da Internet no

Brasil, 2025. Disponível em: https://cartilha.cert.br/. Acesso em: 21 maio 2026.

ESCOLA SUPERIOR DO MINISTÉRIO PÚBLICO DA UNIÃO. Os crimes cibernéticos: aula 1 – governança da internet e crimes cibernéticos. Brasília, DF: ESMPU, 2021. Disponível em: https://escola.mpu.mp.br/plataforma-aprender/acervo-educacional/conteudo/201cinvestigacao-de-crimes-ciberneticos/texto-complementar-aula-1_crimes-ciberneticos-e-governanca_revisao-final-pano-pra-manga_180621.pdf. Acesso em: 21 maio 2026.

FIGUEIREDO, Cléber da Costa; ANTONIOLI, Maria Elisabete; GIL, Patrícia Guimarães. A efetividade de um programa de alfabetização em mídia digital para idosos brasileiros. *Comunicação Mídia e Consumo*, São Paulo, v. 20, n. 58, p. 219-241, 2023. DOI: 10.18568/cmc.v20i58.2792. Disponível em: https://revistacmc.espm.br/revistacmc/article/view/2792. Acesso em: 21 maio 2026.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. As novas configurações dos crimes patrimoniais no Brasil. In: FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. *Anuário Brasileiro de Segurança Pública 2023*. São Paulo: FBSP, 2023. Disponível em: https://forumseguranca.org.br/wp-content/uploads/2023/08/anuario-2023-texto-05-as-novas-configuracoes-dos-crimes-patrimoniais-no-brasil.pdf. Acesso em: 21 maio 2026.

GIL, Antonio Carlos. *Como elaborar projetos de pesquisa*. 7. ed. São Paulo: Atlas, 2022.

IBGE. 161,6 milhões de pessoas com 10 anos ou mais de idade utilizaram a internet no país, em 2022. *Agência de Notícias IBGE*, Rio de Janeiro, 9 nov. 2023. Disponível em: https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/38307-161-6-milhoes-de-pessoas-com-10-anos-ou-mais-de-idade-utilizaram-a-internet-no-pais-em-2022. Acesso em: 21 maio 2026.

HAVERS, Benjamin; TRIPATHI, Kartikeya; BURTON, Alexandra; MARTIN, Wendy; COOPER, Claudia. Exploring the factors preventing older adults from reporting cybercrime

and seeking help: a qualitative, semistructured interview study. *Health & Social Care in the Community*, v. 2024, art. 1314265, 2024. DOI: 10.1155/2024/1314265.Disponível em: https://onlinelibrary.wiley.com/doi/10.1155/2024/1314265. Acesso em: 21 maio 2026.

MENEZES, Matheus Bicca; BORA, Luiz Marcos; ALVES, Maria Laura Vieira. Inclusão digital para idosos: direito humano, prioridade estatal e tendência tecnosocial. *VirtuaJus*, Belo Horizonte, v. 8, n. 15, p. 400-413, 2023. DOI: 10.5752/P.1678-3425.2023v8n15p400-413. Disponível em: https://periodicos.pucminas.br/virtuajus/article/view/32023. Acesso em: 21 maio 2026.

NAIDOO, Rennie. A multi-level influence model of COVID-19 themed cybercrime. *European Journal of Information Systems*, v. 29, n. 3, p. 306-321, 2020. DOI: 10.1080/0960085X.2020.1771222. Disponível em: https://repository.up.ac.za/items/4d749051-1736-4b21-9c27-d4253f7b085c. Acesso em: 21 maio 2026.

PORTES, Letícia Zétola; MARKUS, Jéssica Menzyski. A atualização hermenêutica do fortuito interno bancário: evolução das fraudes no sistema bancário e o dever de vigilância tecnológica à luz do Tema Repetitivo 466/STJ. *Revista Jurídica Gralha Azul – TJPR*, Curitiba, v. 1, n. 32, 2025. DOI: 10.62248/w6wpyg28. Disponível em: https://revista.tjpr.jus.br/gralhaazul/article/view/310. Acesso em: 21 maio 2026.

SHAPIRO, Lauren R. Cyber-enabled imposter scams against older adults in the United States. *Security Journal*, v. 38, art. 43, 2025. DOI: 10.1057/s41284-025-00483-3. Disponível em: https://link.springer.com/article/10.1057/s41284-025-00483-3. Acesso em: 21 maio 2026.

SERRA, Francineia Cartaxo da Silva; MOTA, Laucemir Soares da; NOGUEIRA, Thiago Carlos do Carmo; NASCIMENTO, Marcio de Jesus Lima do. A proteção dos idosos contra crimes cibernéticos no Brasil: desafios e soluções jurídicas. *Revista Ibero-Americana de Humanidades, Ciências e Educação*, v. 11, n. 3, p. 2071-2082, 2025. DOI: 10.51891/rease.v11i3.18570. Disponível em:

https://periodicorease.pro.br/rease/article/view/18570. Acesso em: 21 maio 2026.

VOLPATO, Mariane Spanhol; PEGORARO JUNIOR, Paulo Roberto. Hipervulnerabilidade do idoso em fraudes bancárias eletrônicas. In: ENCONTRO VIRTUAL DO CONPEDI, 7., 2024. *Anais [...]* Florianópolis: CONPEDI, 2024. Disponível em: https://site.conpedi.org.br/publicacoes/v38r977z/033oy6hg/ULWK7vwz0fq5vtQi.pdf. Acesso em: 21 maio 2026.