

ESTELIONATO DIGITAL CONTRA IDOSOS: UMA ANÁLISE SOBRE OS DESAFIOS E A EFETIVAÇÃO DOS DIREITOS DAS VÍTIMAS NO ORDENAMENTO JURÍDICO BRASILEIRO

DIGITAL FRAUD AGAINST THE ELDERLY: AN ANALYSIS OF THE CHALLENGES AND THE EFFECTIVE ENFORCEMENT OF VICTIMS' RIGHTS WITHIN THE BRAZILIAN LEGAL SYSTEM

 <https://doi.org/10.63330/armv2n6-027>

Submetido em: 17/06/2026 e Publicado em: 01/07/2026

Giovane Negreiros dos Santos

Graduando em Direito

Lattes: <http://lattes.cnpq.br/2891648946092390>

Vitória Moreira da Rocha

Graduando em Direito

Lattes: <http://lattes.cnpq.br/8176118400432760>

Álvaro Manoel Nunes Maciel Sobrinho

Bacharel em Direito, Orientador

Lattes: <http://lattes.cnpq.br/1132281725180382>

RESUMO

O presente artigo analisa a efetividade do ordenamento jurídico brasileiro na proteção de pessoas idosas vítimas de estelionato digital, considerando os desafios jurídicos, tecnológicos, institucionais e sociais que atravessam a persecução penal e a reparação civil. A pesquisa adota uma abordagem qualitativa, de caráter exploratório e descritivo, mediante pesquisa bibliográfica e documental, com exame da Constituição Federal, do Estatuto da Pessoa Idosa, do Código Penal, da Lei nº 14.155/2021, Lei nº 15.397/2026, do Marco Civil da Internet, da Lei Geral de Proteção de Dados e de documentos públicos recentes sobre fraudes vinculadas ao INSS. Parte-se da hipótese de que o aumento de pena e a existência de normas protetivas são insuficientes quando não acompanhados de prevenção, governança de dados, educação digital e cooperação interinstitucional. Como resultado, sustenta-se que a pessoa idosa ocupa posição de hipervulnerabilidade no ambiente digital e que a sua proteção demanda resposta jurídica integrada, capaz de articular Direito Penal, Direito Digital, proteção de dados, defesa do consumidor e políticas públicas permanentes.

Palavras-chave: Estelionato digital; Hipervulnerabilidade; Pessoa idosa; Proteção de dados; Reparação integral.



ABSTRACT

This article analyzes the effectiveness of the Brazilian legal system in protecting older persons who are victims of digital fraud, considering legal, technological, institutional and social challenges related to criminal prosecution and civil reparation. The research adopts a qualitative, exploratory and descriptive approach, based on bibliographic and documentary research, including the Federal Constitution, the Older Persons Statute, the Criminal Code, Law nº 14,155/2021, Law nº 15.397/2026, the Brazilian Civil Rights Framework for the Internet, the General Data Protection Law and recent public documents concerning frauds involving INSS beneficiaries. The hypothesis is that higher penalties and protective norms are insufficient without prevention, data governance, digital education and interinstitutional cooperation. The study concludes that older persons are hypervulnerable in digital environments and that their protection requires an integrated legal response involving Criminal Law, Digital Law, data protection, consumer protection and permanent public policies.

Keywords: Comprehensive repair; Data protection; Digital fraud; Elderly person; Hypervulnerability.

1 INTRODUÇÃO

A sociedade contemporânea encontra-se profundamente marcada pela digitalização das relações sociais, econômicas e institucionais. Os serviços bancários, previdenciários, administrativos, comerciais e afetivos passaram a depender das plataformas digitais, dos aplicativos, das autenticações eletrônicas e da circulação permanente de dados pessoais. Essa transformação ampliou o acesso aos direitos e facilitou as rotinas antes burocráticas, mas também deslocou parte relevante da criminalidade para ambientes mediados pela tecnologia. Nesse cenário, o estelionato digital revela-se uma das manifestações mais expressivas da criminalidade patrimonial atual, pois combina a fraude, a engenharia social, a manipulação de dados e a exploração da confiança da vítima.

O recorte deste artigo concentra-se no estelionato digital praticado contra as pessoas idosas, tema que se situa na intersecção entre o Direito Penal, o Direito Digital, a proteção de dados pessoais, o Direito da Pessoa Idosa e as políticas públicas de segurança. A escolha desse objeto decorre da constatação de que a pessoa idosa, embora cada vez mais inserida no ambiente virtual, nem sempre dispõe de um letramento digital suficiente para identificar os riscos, reconhecer as comunicações fraudulentas ou reagir rapidamente às abordagens criminosas. A inclusão digital, quando desacompanhada de uma educação tecnológica, pode converter-se em uma nova forma de exposição.

A relevância social do tema é evidente. Os golpes digitais contra os idosos atingem, simultaneamente, o patrimônio, a autonomia, a dignidade e a segurança subjetiva. Em muitos casos, o valor subtraído corresponde à aposentadoria, à pensão ou ao benefício assistencial utilizado para as despesas



básicas. O dano, portanto, não se esgota na perda financeira; alcança a confiança nas instituições, a autoestima, a saúde emocional e a capacidade de participação social da vítima. A fraude digital, quando direcionada aos idosos, possui uma densidade lesiva agravada, pois incide sobre sujeitos já reconhecidos constitucionalmente como merecedores de uma especial proteção.

No plano jurídico, o tema ganha importância porque o Brasil possui marcos normativos relevantes, mas a sua efetividade prática é frequentemente questionada. A Constituição Federal de 1988 estabelece que a família, a sociedade e o Estado devem amparar as pessoas idosas, assegurando a sua participação na comunidade, a sua dignidade e o seu bem-estar. O Estatuto da Pessoa Idosa reforça essa prioridade. A Lei nº 14.155/2021 agravou a resposta penal ao estelionato praticado por meio eletrônico, movimento recentemente aprofundado pela Lei nº 15.397/2026, que majorou as penas, tipificou a cessão de contas intermediárias e restabeleceu a natureza pública incondicionada da ação penal no estelionato. A LGPD disciplinou o tratamento de dados pessoais. O Marco Civil da Internet estabeleceu os princípios para o uso da rede. Todavia, a existência desses diplomas não impede que as fraudes se multipliquem, sobretudo quando há falhas de prevenção, de fiscalização e de cooperação.

O problema de pesquisa pode ser formulado nos seguintes termos: em que medida o ordenamento jurídico brasileiro é capaz de garantir uma proteção efetiva, uma investigação adequada e uma reparação integral às pessoas idosas vítimas de estelionato digital? A pergunta não busca apenas identificar as normas existentes, mas avaliar a distância entre a proteção formal e a proteção concreta. A investigação parte da premissa de que a tutela jurídica do idoso no ambiente digital deve ser medida não pelo número de leis disponíveis, mas pela capacidade real de prevenir os golpes, identificar os autores, bloquear os valores e restaurar a condição da vítima.

A hipótese central sustenta que, apesar dos avanços normativos, os operadores do Direito enfrentam desafios jurídicos, tecnológicos e institucionais que impedem a plena efetividade da proteção e da reparação. Essa lacuna é agravada pela hipervulnerabilidade da pessoa idosa, pela volatilidade da prova digital, pela fragmentação da atuação estatal, pela insuficiência da educação digital e pela dificuldade de responsabilização de agentes que se ocultam por meio de contas intermediárias, de dispositivos descartáveis, de perfis falsos e de estruturas transnacionais.

O objetivo geral consiste em analisar, sob a ótica jurídico-crítica, a efetividade e as limitações do ordenamento brasileiro na proteção de idosos vítimas de estelionato digital. Os objetivos específicos são: identificar as principais modalidades de fraude digital contra os idosos; examinar as normas aplicáveis; discutir os desafios de investigação, de prova e de reparação; analisar o caso das fraudes relacionadas ao INSS como exemplo de vitimização de aposentados e pensionistas; e propor diretrizes para o aperfeiçoamento legislativo, institucional e preventivo.

A metodologia adotada é qualitativa, exploratória e descritiva. Utiliza-se a pesquisa bibliográfica,



com apoio em autores do Direito Penal, do Direito Digital, da proteção de dados, da criminologia e do envelhecimento, bem como a pesquisa documental, voltada à análise de normas jurídicas, documentos oficiais e informações públicas sobre a Operação Sem Desconto. O método de abordagem é hipotético-dedutivo, pois parte de uma hipótese sobre a insuficiência da proteção formal e busca confrontá-la com o arcabouço normativo e com exemplos concretos.

A estrutura do artigo organiza-se em cinco seções. A primeira discute a criminalidade digital como um fenômeno sociotécnico e a transformação do estelionato tradicional em fraude eletrônica. A segunda examina a vulnerabilidade e a hipervulnerabilidade da pessoa idosa no ambiente digital. A terceira apresenta o arcabouço jurídico brasileiro e suas limitações, contemplando as inovações trazidas pela Lei nº 15.397/2026. A quarta analisa os desafios de efetividade, de investigação e de reparação, incluindo o caso do INSS. A quinta propõe diretrizes de aprimoramento jurídico e institucional. Por fim, as considerações finais retomam a hipótese e apresentam uma síntese conclusiva.

2 CRIMINALIDADE DIGITAL, SOCIEDADE EM REDE E RECONFIGURAÇÃO DO ESTELIONATO

2.1 SOCIEDADE EM REDE E CRIMINALIDADE PATRIMONIAL CONTEMPORÂNEA

A criminalidade digital deve ser compreendida como produto da própria reorganização social provocada pelas tecnologias de informação. A internet não funciona apenas como instrumento neutro, mas como ambiente no qual relações econômicas, identidades, registros, senhas, dados bancários e vínculos institucionais passam a circular. Quando a vida social se torna digitalmente mediada, a criminalidade também se adapta. O estelionato, antes associado a encontros presenciais, documentos físicos e conversas diretas, passa a ocorrer por meio de aplicativos, ligações, mensagens automatizadas, links falsos e páginas que simulam órgãos oficiais¹.

A lógica da sociedade em rede favorece a velocidade da comunicação, mas também amplia a velocidade da fraude. O criminoso pode alcançar inúmeras vítimas em um curto intervalo de tempo, selecionar grupos vulneráveis, testar narrativas e apagar rastros. A fraude deixa de depender apenas da habilidade individual do agente e passa a se apoiar em ecossistemas tecnológicos: bases de dados vazadas, softwares de disparo de mensagens, contas bancárias de passagem, maquininhas, plataformas de pagamento, perfis falsos e interfaces que imitam instituições reconhecidas.

O estelionato digital também revela uma tensão entre inovação tecnológica e capacidade regulatória. O Estado legisla, mas o crime se adapta rapidamente. Novas formas de autenticação geram novas formas de fraude; novas plataformas criam novas superfícies de ataque; novos serviços digitais inserem novos

¹ CASTELLS, Manuel. A sociedade em rede. São Paulo: Paz e Terra, 2020.



públicos no risco. A proteção jurídica, para ser efetiva, precisa combinar norma, prevenção, inteligência investigativa, cooperação com instituições privadas e educação dos usuários². Sem essa combinação, a lei permanece reativa e frequentemente chega depois do dano consumado.

2.2 O TIPO PENAL DO ESTELIONATO E SUA ADAPTAÇÃO AO AMBIENTE ELETRÔNICO

O artigo 171 do Código Penal define o estelionato a partir da obtenção de vantagem ilícita, em prejuízo alheio, mediante artifício, ardil ou qualquer outro meio fraudulento. A estrutura típica revela elementos centrais: fraude, induzimento ou manutenção da vítima em erro, vantagem indevida e dano patrimonial. No ambiente digital, esses elementos permanecem, mas a forma de execução se transforma. O artifício pode ser um link falso; o ardil pode ser uma identidade institucional simulada; o erro pode ocorrer mediante interface que aparenta legitimidade; e a vantagem pode ser obtida por transferência instantânea ou contratação remota.

A Lei nº 14.155/2021 alterou o tratamento penal dos crimes praticados por meio eletrônico, agravando a resposta ao estelionato cometido com o uso de informações fornecidas pela vítima ou por terceiro induzido a erro por redes sociais, contatos telefônicos ou pelo envio de correio eletrônico fraudulento. A alteração legislativa reconhece que o ambiente digital amplia a capacidade lesiva do crime, pois permite escala, anonimato e sofisticação. Contudo, a maior pena não resolve, isoladamente, problemas de autoria, prova, bloqueio de valores e ressarcimento.

No caso das pessoas idosas, a adaptação do estelionato ao ambiente eletrônico adquire gravidade particular. Os golpistas exploram narrativas de urgência, medo, confiança familiar ou autoridade estatal. Mensagens que simulam bancos, previdência, familiares ou servidores públicos são mais eficazes quando atingem vítimas que confiam em comunicações institucionais ou têm dificuldade de verificar a autenticidade. O engano, nesses casos, não decorre de ingenuidade individual, mas de assimetria informacional produzida por sistemas digitais complexos.

A resposta jurídica deve considerar que a fraude digital raramente é ato isolado. Frequentemente envolve cadeia organizada de condutas, desde a obtenção de dados até a dispersão dos valores. Por isso, a persecução penal precisa dialogar com medidas cíveis, administrativas e regulatórias. O Direito Penal atua sobre o agente, mas a proteção da vítima demanda congelamento de valores, contestação bancária, responsabilização de fornecedores negligentes, preservação de provas e atendimento especializado. A dogmática penal, sozinha, não esgota o problema.

² MOTA ALVES, Fabrício da. Investigação e prova digital no Brasil. São Paulo: Atlas, 2022.



2.3 ENGENHARIA SOCIAL, DADOS PESSOAIS E FRAUDE DIRIGIDA

A engenharia social é uma das principais técnicas utilizadas no estelionato digital. Diferentemente de ataques puramente técnicos, ela explora comportamento humano, confiança, medo, desconhecimento e autoridade. O criminoso não precisa invadir sistemas sofisticados quando consegue convencer a própria vítima a entregar senha, código, foto de documento ou confirmação de transação. A fraude torna-se psicológica e informacional, ao valer-se de narrativas cuidadosamente construídas para reduzir a capacidade crítica da pessoa abordada. Nesse sentido, Doneda (2020) destaca que a vulnerabilidade dos usuários no ambiente digital decorre, em grande medida, de assimetrias informacionais e da dificuldade de compreensão sobre o uso de dados pessoais³.

Dados pessoais são o combustível da fraude dirigida. Nome completo, CPF, número de benefício, banco de recebimento, endereço, telefone e informações familiares permitem que o contato pareça legítimo. Quando o golpista demonstra conhecer dados verdadeiros, a vítima tende a acreditar na autenticidade da abordagem. Essa dinâmica revela a conexão entre proteção de dados e prevenção criminal. Como assinala a doutrina, “a proteção de dados somente se torna efetiva quando há governança, transparência e responsabilização na gestão das informações pessoais”⁴. Vazamentos, compartilhamentos inadequados e a ausência de governança ampliam a superfície de vitimização, principalmente de idosos aposentados e pensionistas⁵.

A Lei Geral de Proteção de Dados estabelece princípios como finalidade, adequação, necessidade, segurança e prevenção. Esses princípios têm relevância direta para o enfrentamento do estelionato digital, pois impõem deveres aos agentes que tratam informações pessoais. A proteção de dados não deve ser compreendida apenas como obrigação legal, mas como elemento central da segurança digital contemporânea⁶. Quando bancos, associações, plataformas ou órgãos públicos falham na proteção de dados, não se trata apenas de irregularidade administrativa; cria-se ambiente favorável à fraude, com consequências patrimoniais e existenciais para titulares vulneráveis.

A fraude dirigida contra idosos demonstra que segurança digital não é apenas questão de senha forte. É necessário reduzir a circulação indevida de dados, fiscalizar bases compartilhadas, criar alertas de transações atípicas, simplificar canais de bloqueio e adotar linguagem acessível. A cibersegurança exige abordagem sistêmica, envolvendo tecnologia, governança e educação do usuário⁷. A pessoa idosa não pode ser responsabilizada isoladamente por não compreender mecanismos desenhados para usuários experientes. A prevenção deve ser estrutural e reconhecer que a assimetria técnica é elemento constitutivo da

³ DONEDA, Danilo. Da privacidade à proteção de dados pessoais. São Paulo: Atlas, 2020.

⁴ SCHREIBER, Anderson. Tratamento de dados pessoais e proteção jurídica. Rio de Janeiro: Forense, 2021. p. 66.

⁵ DONEDA, Danilo; WIMMER, Miriam. Regulação de dados pessoais no Brasil. Rio de Janeiro: Forense, 2021.

⁶ PECK, Patrícia. Direito digital brasileiro. 6. ed. São Paulo: Saraiva, 2022.

⁷ VAINZOF, Rony. Cibersegurança e crimes informáticos. São Paulo: Thomson Reuters, 2021.



vulnerabilidade, especialmente em uma sociedade marcada pela digitalização acelerada⁸.

3 PESSOA IDOSA, VULNERABILIDADE E HIPERVULNERABILIDADE DIGITAL

3.1 ENVELHECIMENTO, DIGNIDADE E PRIORIDADE CONSTITUCIONAL

A Constituição Federal atribui à família, à sociedade e ao Estado o dever de amparar as pessoas idosas, assegurando sua participação na comunidade, defendendo sua dignidade e garantindo seu bem-estar. Essa diretriz constitucional não possui caráter meramente simbólico; ela informa todo o sistema jurídico e exige tratamento prioritário em políticas públicas, nos serviços essenciais e nas respostas institucionais. Conforme dispõe o art. 230 da Constituição Federal de 1988:

A família, a sociedade e o Estado têm o dever de amparar as pessoas idosas, assegurando sua participação na comunidade, defendendo sua dignidade e bem-estar e garantindo-lhes o direito à vida.⁹

A dignidade da pessoa humana constitui fundamento estruturante do ordenamento jurídico, devendo orientar a interpretação e a aplicação de todas as normas¹⁰. Assim, quando a pessoa idosa é vítima de fraude digital, a obrigação de proteção deve ser lida à luz desse compromisso constitucional reforçado.

O Estatuto da Pessoa Idosa concretiza essa proteção ao estabelecer prioridade absoluta na efetivação dos direitos fundamentais. A norma parte do reconhecimento de que o envelhecimento pode colocar o indivíduo em uma situação de desigualdade material, exigindo mecanismos compensatórios. Conforme prevê o art. 3º da Lei nº 10.741/2003:

É obrigação da família, da comunidade, da sociedade e do Poder Público assegurar à pessoa idosa, com absoluta prioridade, a efetivação do direito à vida, à saúde, à alimentação, à educação, à cultura, ao esporte, ao lazer, ao trabalho, à cidadania, à liberdade, à dignidade, ao respeito e à convivência familiar e comunitária.¹¹

A igualdade material exige tratamento diferenciado para grupos vulneráveis, a fim de compensar desigualdades estruturais¹². No ambiente digital, essa desigualdade assume formas específicas: dificuldade de navegação em aplicativos, dependência de terceiros para operações bancárias, desconfiança tardia diante de mensagens fraudulentas e barreiras para registrar ocorrências ou contestar transações.

⁸ CASTELLS, Manuel. A sociedade em rede. São Paulo: Paz e Terra, 2020.

⁹ BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 1 jun. 2026.

¹⁰ SARLET, Ingo Wolfgang. A eficácia dos direitos fundamentais. 12. ed. Porto Alegre: Livraria do Advogado, 2012.

¹¹ 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: http://www.planalto.gov.br/ccivil_03/leis/2003/110.741.htm. Acesso em: 1 jun. 2026.

¹² BARROSO, Luís Roberto. Curso de direito constitucional contemporâneo. 6. ed. São Paulo: Saraiva, 2017.



A dignidade da pessoa idosa envolve autonomia, segurança, participação social e a preservação de recursos mínimos de subsistência. O estelionato digital atinge esses elementos simultaneamente. Quando aposentados e pensionistas perdem valores do benefício, sofrem também abalo na própria percepção de controle sobre a vida. Como afirma a doutrina constitucional, “a dignidade da pessoa humana não se restringe à existência física, mas abrange as condições materiais e imateriais necessárias para uma vida digna”¹³. Muitos idosos passam a evitar a tecnologia, desconfiar dos familiares ou sentir vergonha por terem sido enganados. O dano jurídico, portanto, deve ser interpretado em sentido amplo, considerando repercussões materiais e morais¹⁴.

A prioridade constitucional impõe que delegacias, bancos, plataformas e órgãos administrativos desenvolvam fluxos específicos para o atendimento de idosos vítimas de fraude. Não basta disponibilizar canais digitais complexos para quem foi justamente vitimado por meio digital. A proteção efetiva exige linguagem clara, atendimento humano, orientação sobre a preservação de provas, bloqueio célere de valores e encaminhamento integrado. Os direitos fundamentais demandam não apenas abstenções do Estado, mas também prestações positivas eficazes¹⁵. A prioridade legal deve transformar-se em procedimento concreto, sob pena de permanecer como uma promessa abstrata, comprometendo a efetividade do próprio texto constitucional.

3.2 HIPERVULNERABILIDADE COMO CATEGORIA JURÍDICA E SOCIAL

A vulnerabilidade é reconhecida em diversas áreas do Direito, especialmente nas relações de consumo e na proteção de grupos específicos. A hipervulnerabilidade, por sua vez, indica uma situação agravada, na qual diferentes fatores de fragilização se acumulam. No caso da pessoa idosa no ambiente digital, a idade, a baixa familiaridade tecnológica, a dependência de benefícios, o isolamento social e a confiança em comunicações oficiais convergem para ampliar o risco de vitimização. Trata-se de uma vulnerabilidade qualificada, não de uma incapacidade presumida. A vulnerabilidade do consumidor constitui princípio estruturante do sistema jurídico, sendo intensificada em situações específicas, nas quais se verifica a hipervulnerabilidade¹⁶.

É essencial evitar leituras paternalistas. Reconhecer a hipervulnerabilidade da pessoa idosa não significa negar sua autonomia, mas identificar barreiras estruturais que exigem uma proteção reforçada. A dignidade da pessoa humana pressupõe a garantia de condições reais para o exercício da autonomia, o que

¹³ SARLET, Ingo Wolfgang. A eficácia dos direitos fundamentais. 12. ed. Porto Alegre: Livraria do Advogado, 2012. p. 73.

¹⁴ CAVALIERI FILHO, Sérgio. Programa de responsabilidade civil. 15. ed. São Paulo: Atlas, 2021.

¹⁵ MORAES, Alexandre de. Direitos humanos fundamentais. 12. ed. São Paulo: Atlas, 2019.

¹⁶ MARQUES, Cláudia Lima; BENJAMIN, Antônio Herman; MIRAGEM, Bruno. Comentários ao Código de Defesa do Consumidor. 7. ed. São Paulo: Revista dos Tribunais, 2021.



implica o reconhecimento de desigualdades materiais¹⁷. Muitos idosos utilizam a tecnologia com competência, mas o sistema digital é desenhado com velocidade, linguagem e complexidade que podem excluir ou confundir parte significativa desse público. A igualdade material exige um tratamento diferenciado para assegurar condições equitativas de participação social¹⁸. A tutela jurídica deve equilibrar autonomia e proteção, oferecendo instrumentos para que o idoso participe da vida digital sem ser exposto a riscos desproporcionais.

A hipervulnerabilidade também possui uma dimensão informacional. Os golpistas detêm dados, roteiros de persuasão, conhecimento de plataformas e estratégias de ocultação. A vítima, em contrapartida, muitas vezes dispõe apenas da aparência de legitimidade da mensagem recebida. Essa assimetria informacional é um elemento central das relações digitais contemporâneas. O controle sobre dados pessoais constitui fator determinante de poder na sociedade digital, enquanto sua ausência expõe os indivíduos a riscos significativos¹⁹. Essa assimetria é agravada quando a fraude simula um banco, o INSS, um familiar ou uma autoridade pública. Quanto maior a credibilidade social da instituição imitada, maior o poder de convencimento do golpe²⁰.

No plano jurídico, a hipervulnerabilidade deve influenciar a interpretação dos deveres de cuidado. Instituições financeiras, associações, plataformas e órgãos públicos não podem tratar idosos como usuários ordinários em contextos de risco elevado. A responsabilidade civil nas relações de consumo fundamenta-se na teoria do risco do empreendimento, impondo ao fornecedor o dever de segurança²¹. Assim, operações incomuns, contratações remotas, descontos recorrentes e alterações cadastrais envolvendo beneficiários idosos devem acionar camadas adicionais de confirmação. A ausência dessas cautelas pode caracterizar falha do serviço, violação de segurança ou negligência institucional, conforme previsto no Código de Defesa do Consumidor²². A proteção do consumidor vulnerável exige a adoção de medidas preventivas eficazes, especialmente em ambientes digitais de alto risco²³.

3.3 CONSEQUÊNCIAS PATRIMONIAIS, PSICOLÓGICAS E SOCIAIS DA FRAUDE

O dano patrimonial é o aspecto mais visível do estelionato digital. Transferências, empréstimos, descontos indevidos e compras fraudulentas reduzem a renda já comprometida com a alimentação, a saúde, a moradia e os medicamentos. Para aposentados e pensionistas de baixa renda, pequenas quantias podem

¹⁷ SARLET, Ingo Wolfgang. A eficácia dos direitos fundamentais. 12. ed. Porto Alegre: Livraria do Advogado, 2012.

¹⁸ BARROSO, Luís Roberto. Curso de direito constitucional contemporâneo. 6. ed. São Paulo: Saraiva, 2017.

¹⁹ DONEDA, Danilo. Da privacidade à proteção de dados pessoais. São Paulo: Atlas, 2020.

²⁰ PECK, Patrícia. Direito digital brasileiro. 6. ed. São Paulo: Saraiva, 2022.

²¹ CAVALIERI FILHO, Sérgio. Programa de responsabilidade civil. 15. ed. São Paulo: Atlas, 2021.

²² BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: Presidência da República, 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/18078compilado.htm. Acesso em: 1 jun. 2026.

²³ MIRAGEM, Bruno. Curso de direito do consumidor. 9. ed. São Paulo: Revista dos Tribunais, 2022.



representar uma privação significativa. A reparação tardia, quando ocorre, não elimina meses de sofrimento, de endividamento e de insegurança. Por isso, a análise jurídica deve considerar a urgência e a essencialidade dos valores subtraídos, sobretudo quando se trata de verbas de natureza alimentar. A indenização deve buscar recompor integralmente o dano, inclusive em sua dimensão prática e existencial²⁴. Ademais, o Código de Defesa do Consumidor estabelece a responsabilidade objetiva dos fornecedores por falhas na prestação dos serviços, impondo o dever de segurança nas relações de consumo²⁵.

Além do prejuízo material, a fraude produz um dano psicológico. Muitas vítimas relatam vergonha, culpa, medo de utilizar a tecnologia e sensação de incapacidade. O golpe rompe a confiança na própria percepção e pode aprofundar o isolamento social. Em idosos, esse efeito é especialmente sensível, porque a autonomia digital se torna uma condição de acesso aos serviços básicos. O envelhecimento envolve dimensões cognitivas e emocionais que podem influenciar a percepção do risco e a tomada de decisões, tornando a experiência de fraude ainda mais impactante²⁶. A doutrina da responsabilidade civil reconhece que o dano moral abrange não apenas sofrimento psíquico, mas também a violação da dignidade e da autonomia do indivíduo²⁷.

Existe também um dano institucional. Ao serem enganadas por comunicações que simulam bancos, a previdência ou os serviços públicos, as vítimas passam a desconfiar das instituições reais. Essa erosão da confiança prejudica as políticas de inclusão digital, de atendimento remoto e de modernização administrativa. A fraude digital, portanto, não afeta apenas indivíduos; compromete a credibilidade de sistemas públicos e privados que dependem da confiança do usuário para funcionar. A confiança é um elemento essencial na governança digital e na proteção de dados pessoais, sendo sua ruptura um fator de desestabilização social²⁸. A segurança digital deve ser compreendida como uma condição indispensável para o funcionamento das relações institucionais mediadas por tecnologia.²⁹

4 ARCABOUÇO JURÍDICO BRASILEIRO E LIMITAÇÕES DE EFETIVIDADE

4.1 CONSTITUIÇÃO FEDERAL, ESTATUTO DA PESSOA IDOSA E TUTELA PRIORITÁRIA

O Estatuto da Pessoa Idosa reforça a prioridade constitucional ao estabelecer uma proteção integral e um atendimento preferencial. A prioridade deve abranger desde o primeiro contato da vítima com a instituição financeira ou com a delegacia até a eventual ação judicial. O art. 3º da Lei nº 10.741/2003 determina que é dever de todos assegurar ao idoso, com absoluta prioridade, a efetivação dos direitos

²⁴ CAVALIERI FILHO, Sérgio. Programa de responsabilidade civil. 15. ed. São Paulo: Atlas, 2021.

²⁵ BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Código de Defesa do Consumidor. Brasília, DF: Presidência da República, 1990.

²⁶ NERI, Anita Liberalesso. Psicologia do envelhecimento. Campinas: Alínea, 2020.

²⁷ CAVALIERI FILHO, Sérgio. Programa de responsabilidade civil. 15. ed. São Paulo: Atlas, 2021.

²⁸ DONEDA, Danilo. Da privacidade à proteção de dados pessoais. São Paulo: Atlas, 2020.

²⁹ PECK, Patrícia. Direito digital brasileiro. 6. ed. São Paulo: Saraiva, 2022.



fundamentais. Essa diretriz concretiza o comando do art. 230 da Constituição Federal de 1988, que impõe à família, à sociedade e ao Estado o dever de amparar a pessoa idosa, garantindo-lhe a dignidade e o bem-estar. Contudo, a prática revela que muitos canais de contestação são digitais, automatizados e pouco acessíveis. A contradição é evidente: o sistema exige que a vítima de fraude digital resolva o problema por meios digitais, mesmo quando a sua vulnerabilidade decorre justamente desse ambiente. A efetividade dos direitos fundamentais depende de condições reais de acesso, não se satisfazendo com previsões meramente formais³⁰.

A proteção estatutária também deve dialogar com a noção de violência patrimonial. As fraudes digitais que atingem o benefício previdenciário ou a renda de subsistência constituem uma forma de violência econômica contra a pessoa idosa. O Estatuto da Pessoa Idosa, ao tratar das diversas formas de violência, permite uma interpretação sistemática que abrange as práticas que afetem o patrimônio e a autonomia financeira do idoso. Embora o estelionato esteja tipificado no Código Penal, a sua leitura, em casos envolvendo idosos, deve considerar o contexto de especial proteção. A interpretação constitucional exige a consideração das circunstâncias concretas e da posição de vulnerabilidade do sujeito³¹. O bem jurídico tutelado não é apenas o patrimônio abstrato; envolve a segurança existencial, a autonomia e a continuidade das condições mínimas de vida, em consonância com o princípio da dignidade da pessoa humana."

4.2 CÓDIGO PENAL E AS LEIS Nº 14.155/2021 E Nº 15.397/2026

A Lei nº 14.155/2021 representou uma resposta legislativa importante ao reconhecer a maior gravidade dos crimes praticados em ambiente eletrônico (BRASIL, 2021). A qualificação do estelionato digital indica que o legislador percebeu a ampliação da capacidade lesiva da fraude tecnológica. Em termos simbólicos, a norma afirma que o uso da internet, das redes sociais, dos contatos telefônicos e das comunicações eletrônicas para induzir as vítimas ao erro não pode receber um tratamento idêntico ao de fraudes simples e localizadas. A digitalização das relações ampliou o alcance e a escala das fraudes, exigindo respostas normativas específicas³². Recentemente, esse movimento de endurecimento foi aprofundado pela Lei nº 15.397/2026, que promoveu alterações substanciais no Art. 171 do Código Penal, majorando as penas e tipificando condutas acessórias.

A Lei nº 15.397/2026 introduziu a figura da “cessão de conta laranja” no § 2º, VII, criminalizando o ato de ceder conta bancária para o trânsito de recursos ilícitos, e estabeleceu uma nova causa de aumento agravada para a fraude eletrônica no § 2º-A, com pena de reclusão de 4 a 8 anos e multa. Contudo, a

³⁰ SARLET, Ingo Wolfgang. A eficácia dos direitos fundamentais. 12. ed. Porto Alegre: Livraria do Advogado, 2012.

³¹ BARROSO, Luís Roberto. Curso de direito constitucional contemporâneo. 6. ed. São Paulo: Saraiva, 2017.

³² PECK, Patrícia. Direito digital brasileiro. 6. ed. São Paulo: Saraiva, 2022.



mudança mais significativa reside na esfera processual, com a revogação do § 5º do Art. 171. Com essa alteração, a ação penal no crime de estelionato voltou a ser pública incondicionada como regra geral. Essa reversão é fundamental para a proteção de vítimas idosas, pois retira do indivíduo o fardo de representar criminalmente — ato muitas vezes impedido por vergonha ou medo — e devolve ao Estado o protagonismo da persecução penal. Os crimes digitais possuem uma maior complexidade probatória e operacional, o que justifica um tratamento jurídico diferenciado³³.

Apesar disso, o aumento da pena tem um alcance limitado. A função preventiva da pena depende da percepção do risco de identificação e de punição. Em crimes digitais, a impunidade decorre menos da brandura abstrata da pena e mais da dificuldade de investigação. Se os autores não são identificados, se os valores não são bloqueados e se as contas de passagem desaparecem rapidamente, o efeito dissuasório da norma é reduzido. A lei penal precisa ser acompanhada de uma capacidade operacional. Como observa a doutrina especializada, “a efetividade da persecução penal em crimes digitais depende da rapidez na preservação e na análise de evidências eletrônicas”³⁴. Do mesmo modo, a cibercriminalidade se caracteriza pela volatilidade das provas e pela transnacionalidade, fatores que dificultam a atuação estatal³⁵.

Outro ponto crítico é a individualização da conduta. As cadeias criminosas digitais podem envolver os captadores de dados, os operadores de chamada, os criadores de páginas falsas, os intermediários financeiros e os receptadores digitais. A persecução penal deve distinguir os níveis de participação sem perder de vista a organização coletiva. Os modelos tradicionais de autoria, baseados em um ato unitário e presencial, nem sempre captam a dinâmica distribuída da fraude eletrônica. A imputação penal em crimes digitais exige a adaptação dos conceitos clássicos de autoria e de participação, considerando as estruturas organizadas e fragmentadas de execução criminosas³⁶.

A aplicação das Leis nº 14.155/2021 e nº 15.397/2026 a casos envolvendo idosos deve considerar as circunstâncias agravantes e a especial vulnerabilidade da vítima. A fraude praticada contra a pessoa idosa possui uma reprovabilidade aumentada porque explora a confiança, a fragilidade informacional e a dependência econômica. Embora o Código Penal já preveja agravantes relacionadas à idade da vítima, a interpretação judicial deve ser orientada pelos princípios constitucionais de proteção reforçada. A hermenêutica constitucional exige a leitura das normas à luz da dignidade da pessoa humana e da igualdade material³⁷. Nesse sentido, a tecnologia não neutraliza o contato humano; ao contrário, potencializa manipulações dirigidas a públicos específicos, intensificando os riscos para os grupos hipervulneráveis.

³³ BOTTINI, Pierpaolo. Crimes digitais e proteção penal. São Paulo: Revista dos Tribunais, 2023.

³⁴ MOTA ALVES, Fabrício da. Investigação e prova digital no Brasil. São Paulo: Atlas, 2022.

³⁵ VAINZOF, Rony. Cibersegurança e crimes informáticos. São Paulo: Thomson Reuters, 2021.

³⁶ BOTTINI, Pierpaolo. Crimes digitais e proteção penal. São Paulo: Revista dos Tribunais, 2023.

³⁷ BARROSO, Luís Roberto. Curso de direito constitucional contemporâneo. 6. ed. São Paulo: Saraiva, 2017.



4.3 LGPD, MARCO CIVIL DA INTERNET E DEVERES DE SEGURANÇA

A LGPD introduziu no ordenamento brasileiro uma lógica de responsabilização pelo tratamento de dados pessoais. Os seus princípios de finalidade, de adequação, de necessidade, de transparência, de segurança, de prevenção e de responsabilização são diretamente aplicáveis à prevenção das fraudes. Os dados de idosos, especialmente os dados previdenciários e financeiros, devem ser tratados com uma cautela reforçada. Quando as informações circulam sem controle, tornam-se instrumentos da engenharia social e viabilizam golpes personalizados. A proteção de dados pessoais constitui um elemento estruturante da cidadania digital, sendo a sua fragilidade um fator de ampliação dos riscos³⁸. De modo convergente, a doutrina afirma que “a proteção de dados somente se torna efetiva quando há governança, transparência e responsabilização na gestão das informações pessoais”³⁹.

Nessa lógica de responsabilização, ganha relevo o papel da Autoridade Nacional de Proteção de Dados (ANPD), autarquia federal responsável por zelar pela proteção dos dados pessoais e por fiscalizar a aplicação da LGPD. Em contextos de fraude contra idosos, a ANPD desempenha uma função estratégica na apuração dos vazamentos de dados previdenciários, cadastrais e bancários que alimentam golpes personalizados — circunstância exemplificada por episódios de divulgação massiva de bases do INSS, do CadÚnico e das instituições financeiras. A atuação da Autoridade inclui a investigação de incidentes de segurança, a aplicação de sanções administrativas (advertência, multa simples e diária, publicização da infração, suspensão e proibição do tratamento), a edição de regulamentos sobre relatórios de impacto e de governança, além de uma atuação cooperativa com o Ministério Público, os Procons, o Banco Central, o INSS e os órgãos de defesa do consumidor. Em casos como o da Operação Sem Desconto, a articulação entre a ANPD, a CGU, a AGU e a Polícia Federal mostra-se decisiva para conectar o uso indevido de dados pessoais à cadeia de descontos não autorizados em benefícios previdenciários, evidenciando que a proteção de dados não é um tema apartado da proteção penal, mas uma camada preventiva da própria tutela patrimonial dos hipervulneráveis⁴⁰.

O princípio da segurança exige medidas técnicas e administrativas aptas a proteger os dados pessoais contra os acessos não autorizados e contra as situações acidentais ou ilícitas. Já o princípio da prevenção impõe a adoção de medidas para evitar os danos antes que eles ocorram. Em um contexto de estelionato digital, esses princípios autorizam a exigência, junto aos agentes públicos e privados, de protocolos antifraude, de registros auditáveis, de limitação de acesso interno, de uma autenticação robusta e de uma resposta rápida a incidentes. A segurança da informação deve ser tratada como um componente essencial

³⁸ DONEDA, Danilo. Da privacidade à proteção de dados pessoais. São Paulo: Atlas, 2020.

³⁹ SCHREIBER, Anderson. Tratamento de dados pessoais e proteção jurídica. Rio de Janeiro: Forense, 2021. p. 66.

⁴⁰ BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD), arts. 55-A a 55-L. Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em: 1 jun. 2026.



das atividades econômicas e institucionais, especialmente em ambientes digitais de alto risco⁴¹. Assim, a proteção de dados não é um tema apartado da proteção penal; é uma camada preventiva da própria tutela patrimonial.

O Marco Civil da Internet estabelece os direitos, as garantias e os deveres no uso da rede, incluindo a proteção da privacidade e dos dados pessoais. Também disciplina a guarda dos registros de conexão e de acesso às aplicações, bem como a cooperação com as autoridades mediante ordem judicial. Embora seja importante, o marco enfrenta desafios diante da velocidade da fraude digital. Muitas vezes, quando a vítima busca as providências, os registros já foram apagados, as contas foram encerradas ou os valores foram rapidamente movimentados. A prova digital é volátil e depende de uma rápida preservação para manter a sua integridade⁴². Nessa perspectiva, a efetividade da resposta estatal depende da integração entre a tecnologia, a investigação e a cooperação institucional⁴³.

A articulação entre a LGPD, o Marco Civil da Internet e o Direito Penal permite construir uma resposta mais completa ao estelionato digital. O crime deve ser investigado, mas também é necessário apurar se houve uma falha de segurança, um vazamento de dados ou um tratamento indevido que facilitaram a fraude. Em situações que envolvem as vítimas idosas, essa análise deve ser ainda mais rigorosa, considerando a hipervulnerabilidade do grupo. A responsabilidade civil nas relações de consumo fundamenta-se na teoria do risco do empreendimento, impondo ao fornecedor o dever de garantir uma segurança adequada⁴⁴. Assim, a pergunta jurídica não deve se limitar à identificação do autor do crime, mas deve abranger também a verificação das condutas omissivas ou das falhas institucionais que permitiram a circulação indevida dos dados e a realização das operações suspeitas.

4.4 DIREITO DO CONSUMIDOR, INSTITUIÇÕES FINANCEIRAS E RESPONSABILIDADE CIVIL

Muitos golpes digitais contra idosos ocorrem em um contexto bancário ou de contratação de crédito. Nesses casos, o Código de Defesa do Consumidor desempenha um papel central, pois reconhece a vulnerabilidade do consumidor e impõe a responsabilidade objetiva ao fornecedor por falhas na prestação dos serviços. As instituições financeiras integram essa lógica, conforme o entendimento consolidado do Superior Tribunal de Justiça na Súmula 297, segundo a qual “o Código de Defesa do Consumidor é aplicável às instituições financeiras”⁴⁵. Assim, devem responder quando a fraude se relaciona à deficiência de segurança, à ausência de verificação adequada ou à contratação não autorizada. Nessa perspectiva, a

⁴¹ PECK, Patrícia. Direito digital brasileiro. 6. ed. São Paulo: Saraiva, 2022.

⁴² MOTA ALVES, Fabrício da. Investigação e prova digital no Brasil. São Paulo: Atlas, 2022.

⁴³ VAINZOF, Rony. Cibersegurança e crimes informáticos. São Paulo: Thomson Reuters, 2021.

⁴⁴ CAVALIERI FILHO, Sérgio. Programa de responsabilidade civil. 15. ed. São Paulo: Atlas, 2021.

⁴⁵ BRASIL. Superior Tribunal de Justiça. Súmula nº 297. O Código de Defesa do Consumidor é aplicável às instituições financeiras. Segunda Seção, julgada em 12 maio 2004. Diário da Justiça, Brasília, DF, 9 set. 2004, p. 149.



responsabilidade civil nas relações de consumo fundamenta-se no dever de segurança, sendo desnecessária a comprovação da culpa do fornecedor⁴⁶.

A responsabilidade civil em fraudes bancárias digitais deve observar o risco da atividade. Os bancos lucram com a digitalização, a automação, o crédito remoto e a redução do atendimento presencial. Não podem transferir integralmente ao consumidor idoso o custo dos riscos criados por esse modelo. Conforme dispõe o art. 14 do Código de Defesa do Consumidor, o fornecedor responde, independentemente de culpa, pelos danos causados por defeitos relativos à prestação dos serviços. O risco do empreendimento impõe ao fornecedor o dever de prever e de mitigar os riscos inerentes à sua atividade econômica⁴⁷. Se a instituição oferece contratação por aplicativo, a autenticação remota e a movimentação instantânea, deve implementar mecanismos proporcionais de prevenção, de monitoramento e de bloqueio.

Em casos de empréstimos consignados, de descontos associativos ou de contratações remotas, a prova do consentimento deve ser robusta. A simples existência de um registro interno não basta quando a vítima nega a autorização e se encontra em uma situação de hipervulnerabilidade. As assinaturas eletrônicas, as gravações, a biometria, os logs e as confirmações devem ser auditáveis. A proteção do consumidor vulnerável exige as garantias de transparência e de segurança na formação do vínculo contratual⁴⁸. Ademais, a rastreabilidade e a integridade dos dados são essenciais para garantir a validade das operações digitais⁴⁹. A dúvida razoável sobre o consentimento deve favorecer a proteção do idoso, especialmente quando há um padrão massivo de reclamações ou indícios de uma fraude estrutural, em observância ao princípio da boa-fé objetiva.

A reparação integral exige a restituição dos valores, o cancelamento dos contratos indevidos, a correção monetária, uma eventual indenização por dano moral e a adoção de medidas para evitar a reincidência. O dano moral não deve ser banalizado, mas tampouco ignorado quando a fraude compromete o benefício alimentar, gera ansiedade e impõe uma peregrinação institucional. Conforme assinala a doutrina, “o dano moral caracteriza-se pela violação dos direitos da personalidade, atingindo a esfera íntima do indivíduo”⁵⁰. A pessoa idosa submetida a descontos indevidos ou endividamento fraudulento sofre uma violação que ultrapassa o mero aborrecimento, configurando uma lesão à dignidade da pessoa humana, princípio fundamental do ordenamento jurídico⁵¹.

Nesse contexto, ganha especial relevância a Teoria do Desvio Produtivo do Consumidor, formulada por Marcos Dessaune, segundo a qual o tempo de vida da vítima, desperdiçado em razão das falhas dos

⁴⁶ CAVALIERI FILHO, Sérgio. Programa de responsabilidade civil. 15. ed. São Paulo: Atlas, 2021.

⁴⁷ MIRAGEM, Bruno. Curso de direito do consumidor. 9. ed. São Paulo: Revista dos Tribunais, 2022.

⁴⁸ MARQUES, Cláudia Lima; BENJAMIN, Antônio Herman; MIRAGEM, Bruno. Comentários ao Código de Defesa do Consumidor. 7. ed. São Paulo: Revista dos Tribunais, 2021.

⁴⁹ DONEDA, Danilo. Da privacidade à proteção de dados pessoais. São Paulo: Atlas, 2020.

⁵⁰ CAVALIERI FILHO, Sérgio. Programa de responsabilidade civil. 15. ed. São Paulo: Atlas, 2021. p. 118.

⁵¹ SARLET, Ingo Wolfgang. A eficácia dos direitos fundamentais. 12. ed. Porto Alegre: Livraria do Advogado, 2012.



fornecedores e da necessidade de buscar, por meios próprios, a solução dos problemas a que não deu causa, constitui um dano autônomo e indenizável. A pessoa idosa que, após sofrer estelionato digital ou descontos não autorizados, vê-se obrigada a “peregrinar” entre as agências bancárias, as delegacias, os postos do INSS, os Procons, a Defensoria Pública e o Judiciário — muitas vezes utilizando os mesmos canais digitais que a vitimaram — sofre uma perda significativa de tempo útil, qualificada pela sua condição de hipervulnerabilidade. Trata-se de um acréscimo (*plus*) em relação ao dano moral tradicional, que se soma à violação da dignidade, à angústia e ao comprometimento do orçamento alimentar. A aplicação dessa teoria às vítimas idosas reforça o dever das instituições financeiras e dos órgãos públicos de criar fluxos prioritários, um atendimento humanizado e uma resposta célere, sob pena de o próprio sistema de proteção converter-se em uma fonte adicional de lesão, agravando o dano moral já configurado⁵².

5 DESAFIOS DE INVESTIGAÇÃO, PROVA, REPARAÇÃO E O CASO INSS

5.1 PROVA DIGITAL E PERSECUÇÃO PENAL

A prova digital possui características próprias: é volátil, replicável, alterável e frequentemente armazenada por terceiros. As capturas de tela (*prints*) de conversa, embora úteis, podem ser questionadas; os registros de acesso dependem de provedores; os dados bancários exigem cooperação institucional; e o rastreamento de valores precisa ocorrer rapidamente. Em um estelionato digital contra idosos, o tempo é um fator decisivo. Cada hora de demora aumenta a probabilidade de dispersão dos recursos por contas intermediárias. Como destaca a doutrina, “a prova digital demanda imediata preservação, sob pena de perda irreversível de elementos essenciais à investigação”⁵³. Nessa mesma linha, a volatilidade das evidências digitais impõe respostas céleres e tecnicamente qualificadas por parte das autoridades⁵⁴.

O boletim de ocorrência deve ser apenas o início de uma cadeia de preservação probatória. A vítima precisa ser orientada a guardar mensagens, números de telefone, comprovantes, links, protocolos, extratos e eventuais gravações. As delegacias devem possuir fluxos padronizados para requerer informações aos bancos e aos provedores. O Código de Processo Penal, ao tratar da cadeia de custódia (arts. 158-A a 158-F), reforça a necessidade de preservação da integridade dos vestígios. Sem uma padronização, a investigação depende da iniciativa individual dos agentes, o que produz uma desigualdade territorial e institucional. A ausência de protocolos uniformes compromete a eficiência da persecução penal em crimes digitais.⁵⁵

A autoria é um dos maiores entraves. Muitos golpes utilizam contas bancárias em nome de terceiros,

⁵² DESSAUNE, Marcos. Teoria aprofundada do desvio produtivo do consumidor: o prejuízo do tempo desperdiçado e da vida alterada. 3. ed. Vitória: Edição do Autor, 2022.

⁵³ MOTA ALVES, Fabrício da. Investigação e prova digital no Brasil. São Paulo: Atlas, 2022.

⁵⁴ VAINZOF, Rony. Cibersegurança e crimes informáticos. São Paulo: Thomson Reuters, 2021.

⁵⁵ LIMA, Katia S. P. Crimes digitais: desafios e tendências. São Paulo: Saraiva, 2023.



documentos falsos, chips pré-pagos e perfis descartáveis. A pessoa que recebe o valor pode alegar desconhecimento ou ter sido cooptada. Ainda assim, o rastreamento financeiro continua sendo um caminho relevante, pois revela redes de movimentação. A imputação penal em crimes digitais deve considerar estruturas organizadas e fragmentadas, superando modelos tradicionais centrados na autoria individual direta⁵⁶. O enfrentamento eficaz exige a integração entre a inteligência financeira, a polícia judiciária, o Ministério Público e as instituições privadas.⁵⁷

Um obstáculo investigativo cada vez mais frequente é a conversão dos valores subtraídos em criptoativos. Após o golpe, os recursos costumam transitar por uma cadeia de contas-laranja e, em seguida, são utilizados para a compra de criptomoedas em corretoras (*exchanges*) nacionais e estrangeiras, sendo posteriormente fracionados, transferidos entre múltiplas carteiras (*wallets*) e, em alguns casos, “lavados” por meio de *mixers*, *tumblers* e *exchanges* descentralizadas. Essa dinâmica configura um ciclo típico de lavagem de dinheiro, conforme o art. 1º da Lei nº 9.613/1998⁵⁸, e dificulta a recuperação dos valores em razão da pseudonímia das transações, da transnacionalidade da *blockchain* e da rapidez das operações. A persecução penal em estelionato digital contra idosos depende, portanto, do desenvolvimento de capacidades técnicas em *blockchain forensics* pelas forças de segurança e pelo Ministério Público, incluindo o uso de ferramentas de análise *on-chain*, a cooperação com a Receita Federal, o Banco Central, o COAF (Conselho de Controle de Atividades Financeiras) e as *exchanges*, além da articulação internacional para o bloqueio e a repatriação de ativos. A própria regulamentação dos prestadores de serviços de ativos virtuais, no contexto da Lei nº 14.478/2022, deve dialogar com a proteção das vítimas hipervulneráveis, exigindo dos operadores um cadastro qualificado, o monitoramento de transações atípicas e uma cooperação rápida com as autoridades⁵⁹.

5.2 REPARAÇÃO INTEGRAL E BLOQUEIO DE VALORES

A reparação integral é uma das dimensões mais frágeis da tutela das vítimas. Mesmo quando o boletim é registrado e a investigação avança, os valores frequentemente já foram sacados, transferidos ou convertidos. Para os idosos, essa demora é especialmente grave porque o montante subtraído pode ter natureza alimentar. A efetividade da proteção deve ser medida pela capacidade de impedir a consolidação do dano, não apenas pela abertura de uma investigação posterior. A reparação civil deve ser integral,

⁵⁶ BOTTINI, Pierpaolo. Crimes digitais e proteção penal. São Paulo: Revista dos Tribunais, 2023.

⁵⁷ VAINZOF, Rony. Cibersegurança e crimes informáticos. São Paulo: Thomson Reuters, 2021.

⁵⁸ BRASIL. Lei nº 9.613, de 3 de março de 1998. Dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; cria o Conselho de Controle de Atividades Financeiras - COAF. Brasília, DF: Presidência da República, 1998. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/19613compilado.htm. Acesso em: 02 jun. 2026.

⁵⁹ BRASIL. Lei nº 14.478, de 21 de dezembro de 2022. Dispõe sobre diretrizes a serem observadas na prestação de serviços de ativos virtuais e na regulamentação das prestadoras de serviços de ativos virtuais. Brasília, DF: Presidência da República, 2022. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/lei/14478.htm. Acesso em: 1 jun. 2026.



abrangendo todas as consequências do dano, inclusive aquelas de natureza prática e existencial⁶⁰. Nesse sentido, a tutela jurídica deve priorizar medidas que preservem o patrimônio da vítima antes que ele seja definitivamente dissipado.

Essa noção de integralidade deve ser lida em conjunto com a Teoria do Desvio Produtivo do Consumidor, que reconhece como um dano autônomo o tempo de vida desperdiçado pela vítima na tentativa de solucionar problemas a que não deu causa. Para a pessoa idosa vítima de estelionato digital, esse desvio produtivo se manifesta em filas, atendimentos repetitivos, deslocamentos a delegacias e a órgãos previdenciários, sucessivos contatos com call centers automatizados e ações judiciais demoradas — tudo em uma fase em que o tempo restante de vida é, por definição, um recurso escasso e qualificado. A indenização deve, portanto, recompor não apenas o patrimônio subtraído e o abalo moral, mas também o tempo útil consumido por uma falha de serviço⁶¹.

Medidas de bloqueio cautelar devem ser ágeis e acessíveis. As instituições financeiras precisam manter canais de contestação imediata, com um atendimento humanizado para os idosos. O Judiciário deve apreciar os pedidos urgentes considerando a vulnerabilidade da vítima e a velocidade das transações digitais. O Código de Processo Civil prevê a tutela de urgência quando há probabilidade do direito e perigo de dano ou risco ao resultado útil do processo. A tutela de urgência deve ser concedida sempre que a demora processual puder tornar ineficaz a proteção jurisdicional⁶². Assim, a demora processual, em matéria de fraude eletrônica, pode equivaler à perda definitiva do direito, exigindo uma atuação judicial célere e eficaz.

A reparação civil também enfrenta obstáculos probatórios. Os bancos podem atribuir a culpa exclusiva à vítima, alegando o fornecimento voluntário de senha ou de código. Essa tese precisa ser examinada com cautela quando há uma engenharia social sofisticada e uma hipervulnerabilidade. O Código de Defesa do Consumidor estabelece a responsabilidade objetiva do fornecedor, admitindo a sua exclusão apenas quando comprovada a culpa exclusiva da vítima. Contudo, essa excludente deve ser interpretada restritivamente, especialmente em contextos de vulnerabilidade acentuada⁶³. A conduta da vítima não deve ser avaliada por um padrão abstrato de usuário experiente, mas por critérios concretos de acessibilidade, de clareza da comunicação, de risco da atividade e de dever de prevenção do fornecedor.

5.3 A OPERAÇÃO SEM DESCONTO E AS FRAUDES VINCULADAS AO INSS

O caso das fraudes relacionadas ao INSS oferece um exemplo concreto da vulnerabilidade de aposentados e pensionistas diante de estruturas que combinam dados pessoais, confiança institucional e

⁶⁰ CAVALIERI FILHO, Sérgio. Programa de responsabilidade civil. 15. ed. São Paulo: Atlas, 2021.

⁶¹ DESSAUNE, Marcos. Teoria aprofundada do desvio produtivo do consumidor: o prejuízo do tempo desperdiçado e da vida alterada. 3. ed. Vitória: Edição do Autor, 2022.

⁶² DIDIER JR., Fredie et al. Curso de direito processual civil. Salvador: JusPodivm, 2021.

⁶³ MIRAGEM, Bruno. Curso de direito do consumidor. 9. ed. São Paulo: Revista dos Tribunais, 2022.



descontos automáticos. Em 23 de abril de 2025, a Controladoria-Geral da União informou a deflagração da Operação Sem Desconto, em conjunto com a Polícia Federal, para apurar descontos associativos realizados diretamente em benefícios previdenciários. Segundo a CGU, o relatório indicou que mais de 97% dos beneficiários entrevistados não autorizaram os descontos, e o impacto financeiro poderia alcançar R\$ 6,3 bilhões⁶⁴. Esse dado evidencia a magnitude do problema e sua relevância jurídica e social.

A gravidade do caso está no fato de que a vítima não precisava necessariamente clicar em um link falso ou realizar uma transferência espontânea. A fraude estaria relacionada aos descontos em folha de aposentados e pensionistas, com base em acordos e autorizações questionadas. Isso demonstra que o estelionato e as fraudes patrimoniais contemporâneas podem ocorrer por meio de estruturas formalmente institucionais, nas quais a aparência de legalidade dificulta a percepção do dano pela pessoa idosa. A vulnerabilidade do consumidor se intensifica quando a prática abusiva se oculta sob a aparência de regularidade contratual, dificultando a identificação da irregularidade⁶⁵.

A CGU também apontou fragilidades documentais e recomendou medidas como o bloqueio cautelar de novos descontos e o aprimoramento dos procedimentos de formalização, de execução, de suspensão e de cancelamento de acordos. Esse dado é relevante para o presente artigo porque evidencia que a prevenção de fraudes contra idosos depende de uma governança administrativa. Não basta punir depois; é necessário impedir que sistemas de desconto, crédito, associação ou consignação operem sem uma verificação rigorosa de consentimento. A governança de dados e a rastreabilidade das operações são essenciais para prevenir abusos e garantir a segurança jurídica⁶⁶.

O caso do INSS também se conecta diretamente à proteção de dados pessoais. Para que os descontos ou as abordagens fraudulentas alcancem beneficiários específicos, os dados previdenciários e cadastrais tornam-se elementos sensíveis da fraude. A Lei Geral de Proteção de Dados estabelece deveres de segurança e prevenção no tratamento dessas informações. O controle sobre dados pessoais constitui um elemento central na proteção do indivíduo na sociedade digital⁶⁷. A pessoa idosa confia no benefício porque ele provém do Estado. Quando seu contracheque previdenciário sofre um desconto indevido ou quando golpistas utilizam informações relacionadas ao INSS para abordá-la, a violação atinge não apenas o patrimônio, mas também a confiança pública e institucional.

Em dezembro de 2025, a Advocacia-Geral da União divulgou medidas judiciais de bloqueio de bens de investigados para o ressarcimento de aposentados e pensionistas, informando liminares relacionadas a

⁶⁴ BRASIL. Controladoria-Geral da União. Operação combate descontos não autorizados de aposentados e pensionistas; valor pode chegar a R\$ 6,3 bi. Brasília, DF, 23 abr. 2025. Disponível em: <https://www.gov.br/cgu/pt-br/assuntos/noticias>. Acesso em: 1 jun. 2026.

⁶⁵ MIRAGEM, Bruno. Curso de direito do consumidor. 9. ed. São Paulo: Revista dos Tribunais, 2022.

⁶⁶ SCHREIBER, Anderson. Tratamento de dados pessoais e proteção jurídica. Rio de Janeiro: Forense, 2021.

⁶⁷ DONEDA, Danilo. Da privacidade à proteção de dados pessoais. São Paulo: Atlas, 2020.



valores bilionários⁶⁸. A atuação da AGU demonstra que a reparação coletiva pode exigir instrumentos cautelares robustos, a indisponibilidade patrimonial e a coordenação entre órgãos de controle, de segurança pública e de representação judicial do Estado. Ainda assim, o ressarcimento posterior não elimina a necessidade de prevenção.

Além disso, a dimensão coletiva do caso revela falhas sistêmicas. Quando o dano decorre de uma falha estrutural na prestação do serviço, a responsabilidade pode ultrapassar o caso individual, alcançando o dever de reparação e de prevenção em escala ampliada⁶⁹. O episódio reforça que a tutela jurídica dos idosos no ambiente digital exige a integração entre o direito do consumidor, a proteção de dados e a responsabilidade administrativa. A fraude não deve ser analisada apenas como um evento isolado, mas como um sintoma de fragilidade institucional que demanda respostas estruturais e preventivas.

5.4 O CASO INSS COMO PARADIGMA DE ANÁLISE JURÍDICA

O exemplo do caso do INSS é paradigmático porque revela múltiplas camadas do problema. Em primeiro lugar, evidencia a vulnerabilidade econômica de aposentados e pensionistas, pois descontos aparentemente pequenos podem comprometer a renda de subsistência. Em segundo lugar, demonstra a centralidade dos dados pessoais e previdenciários. Em terceiro lugar, expõe fragilidades de governança nos sistemas de autorização e de desconto. Em quarto lugar, mostra que a reparação depende de uma ação coletiva e institucional, não apenas de iniciativas individuais das vítimas.

Esse caso também permite diferenciar a fraude digital em sentido estrito e a fraude em contexto digitalizado. Nem toda vitimização de idosos decorre de invasão de dispositivo ou clique em link. Muitas fraudes resultam de uma digitalização administrativa mal governada, consentimentos frágeis, bases de dados expostas e procedimentos automatizados. Por isso, a análise jurídica não deve restringir o estelionato digital ao computador da vítima; ela deve alcançar a infraestrutura que permite a circulação e a monetização indevida de informações.

Sob a ótica penal, é necessário apurar quem obteve vantagem ilícita, quem viabilizou os descontos, quem falsificou ou simulou autorizações e quem se beneficiou economicamente. Sob a ótica civil, impõe-se assegurar a restituição e a indenização quando cabível. Sob a ótica administrativa, cabe revisar os contratos, os acordos, os protocolos e os mecanismos de fiscalização. Sob a ótica da proteção de dados, deve-se investigar as bases utilizadas, os acessos indevidos e as medidas de segurança adotadas.

⁶⁸ BRASIL. Advocacia-Geral da União. AGU obtém bloqueio de mais R\$ 500 milhões para ressarcir aposentados e pensionistas. Brasília, DF, 17 dez. 2025. Disponível em: <https://www.gov.br/agu/pt-br/comunicacao/noticias>. Acesso em: 1 jun. 2026.

⁶⁹ CAVALIERI FILHO, Sérgio. Programa de responsabilidade civil. 15. ed. São Paulo: Atlas, 2021.



6 CITAÇÕES DIRETAS ESTRATÉGICAS, ANÁLISE CRÍTICA E PROPOSTAS

6.1 CITAÇÕES NORMATIVAS ESTRATÉGICAS E SUA INTERPRETAÇÃO

A primeira citação estratégica decorre da Constituição Federal. O artigo 230 dispõe que “a família, a sociedade e o Estado têm o dever de amparar as pessoas idosas”. Essa fórmula constitucional é essencial porque impede uma leitura restrita da proteção. O dever não é exclusivo da família, nem apenas do Estado; é compartilhado. Em matéria digital, isso significa que as plataformas, os bancos, as associações, os órgãos públicos e a comunidade possuem responsabilidades na prevenção de fraudes e no acolhimento da vítima.

O Estatuto da Pessoa Idosa estabelece, em seu artigo 3º, que é obrigação da família, da comunidade, da sociedade e do poder público assegurar à pessoa idosa, com absoluta prioridade, a efetivação dos direitos fundamentais. A expressão “absoluta prioridade” deve ser interpretada como um comando de preferência real. No contexto do estelionato digital, ela exige um atendimento célere, uma linguagem acessível, a prioridade na contestação de transações, uma tramitação eficiente e a proteção contra a revitimização burocrática.

A LGPD, ao prever o princípio da segurança, exige a utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações ilícitas. Essa previsão é estratégica porque conecta a proteção de dados e a prevenção penal. Quando os dados de idosos são tratados sem segurança, aumenta o risco de golpes personalizados. A violação de dados pode ser uma etapa anterior do estelionato, ainda que a subtração patrimonial ocorra depois por contato telefônico, aplicativo ou desconto indevido.

O Código Penal, ao tratar do estelionato, fala em artifício, artil ou qualquer outro meio fraudulento. A amplitude da expressão permite enquadrar novas formas de manipulação digital sem a necessidade de criar um tipo penal para cada tecnologia. O desafio não é apenas tipificar, mas também provar. A dogmática penal possui uma elasticidade suficiente para alcançar a fraude eletrônica; a lacuna principal reside na efetividade investigativa e na capacidade de reparação.

6.2 PROPOSTAS DE APRIMORAMENTO LEGISLATIVO

Uma primeira proposta consiste em reconhecer expressamente, em legislação específica ou em alteração normativa, protocolos reforçados para a contratação digital envolvendo pessoas idosas. Os empréstimos consignados, os descontos associativos, as alterações cadastrais e as autorizações recorrentes deveriam exigir uma confirmação qualificada, uma linguagem simples, um registro auditável e a possibilidade de cancelamento facilitado. A proteção não deve impedir a contratação, mas garantir um consentimento livre, informado e verificável.

Também seria recomendável criar um dever legal de comunicação imediata de operações suspeitas envolvendo idosos. Os bancos e as instituições financeiras já dispõem de sistemas de monitoramento de



risco. Tais sistemas devem considerar a idade, o padrão histórico de transações, o destino incomum de valores e a contratação atípica. Quando houver um indício de fraude, a operação poderia ser temporariamente bloqueada para a confirmação por um canal seguro, sem prejuízo da autonomia do usuário.

Outra medida legislativa relevante seria fortalecer os mecanismos de restituição administrativa. A vítima idosa não deveria depender exclusivamente de uma ação judicial para reaver valores evidentemente indevidos. Procedimentos administrativos com prazos curtos, a inversão do ônus de comprovação do consentimento e a fiscalização por órgãos de defesa do consumidor poderiam reduzir os danos. Em fraudes massivas, os modelos coletivos de ressarcimento são mais adequados do que milhares de demandas individuais.

No campo penal, o aprimoramento deve priorizar os instrumentos investigativos e não apenas o aumento de pena. Os prazos de preservação de registros, os canais padronizados de cooperação, o treinamento de policiais e a integração com a inteligência financeira têm um maior potencial preventivo. A experiência demonstra que penas abstratas elevadas não bastam se a chance de identificação é baixa. O Direito Penal precisa ser operacionalmente viável.

6.3 PROPOSTAS INSTITUCIONAIS E TECNOLÓGICAS

O fortalecimento de delegacias especializadas em crimes cibernéticos é uma medida indispensável, mas não suficiente. É necessário capacitar também as delegacias comuns, pois as vítimas idosas frequentemente procuram a unidade mais próxima. O primeiro atendimento deve ser capaz de orientar a preservação de provas, acionar mecanismos de bloqueio e encaminhar o caso adequadamente. A especialização não pode gerar uma concentração inacessível, sobretudo em regiões periféricas e no interior.

As instituições financeiras devem criar canais prioritários para idosos vítimas de golpe, com um atendimento humano e um protocolo de urgência. A automação excessiva pode revitimizar. Um idoso que acabou de sofrer uma fraude não deve enfrentar menus eletrônicos confusos, respostas padronizadas e exigências documentais repetidas. O atendimento deve combinar acolhimento, bloqueio preventivo, explicação clara e a produção de provas para uma eventual investigação.

Os órgãos previdenciários e assistenciais precisam investir em uma comunicação pública permanente. Os alertas sobre golpes devem ser simples, repetidos e distribuídos por canais que alcancem os idosos: rádio, televisão, unidades de saúde, CRAS, bancos, igrejas, associações comunitárias e aplicativos oficiais. A comunicação não pode pressupor que todos acompanham os portais eletrônicos. Uma educação digital eficaz é aquela que chega ao cotidiano da população vulnerável.

Tecnologicamente, recomenda-se a adoção de uma autenticação multifatorial acessível, biometria com cautelas, confirmação ativa de consentimento e trilhas de auditoria. Contudo, a tecnologia não deve



ser confundida com exclusão. Os sistemas de segurança precisam considerar limitações da visão, da audição, da memória, da escolaridade e do acesso à internet. A solução antifraude que só funciona para usuários avançados reproduz a desigualdade e pode afastar os idosos de serviços essenciais.

7 CONSIDERAÇÕES FINAIS

A presente investigação buscou analisar a efetividade do ordenamento jurídico brasileiro na proteção das pessoas idosas vítimas de estelionato digital. Partiu-se da constatação de que a digitalização das relações sociais e econômicas ampliou o acesso aos serviços, mas também criou novas oportunidades para a criminalidade patrimonial. A pessoa idosa, inserida nesse ambiente muitas vezes sem uma preparação adequada, torna-se um alvo preferencial de golpes que exploram a confiança, o medo, a autoridade e a assimetria informacional.

O estudo demonstrou que o estelionato digital não é uma mera versão tecnológica de uma fraude antiga. Trata-se de um fenômeno complexo, estruturado por meio dos dados pessoais, da engenharia social, das plataformas digitais, dos sistemas financeiros instantâneos e das redes de ocultação. A fraude eletrônica possui uma escala, uma velocidade e uma capacidade de dispersão que desafiam a investigação tradicional. Quando praticada contra os idosos, a sua gravidade é ampliada pela natureza alimentar dos recursos atingidos e pelas consequências psicológicas e sociais produzidas.

A análise normativa revelou que o Brasil dispõe de instrumentos importantes. A Constituição Federal estabelece um dever compartilhado de amparo às pessoas idosas. O Estatuto da Pessoa Idosa assegura a prioridade e a proteção integral. O Código Penal tipifica o estelionato, tendo sido substancialmente aprimorado pelas Leis nº 14.155/2021 e nº 15.397/2026. Esta última, ao estabelecer uma nova causa de aumento agravada para a fraude eletrônica, tipificar a cessão de conta laranja e restabelecer a natureza pública incondicionada da ação penal, representou um avanço crucial para a proteção de vítimas hipervulneráveis. De modo convergente, a LGPD impõe os deveres de segurança e de prevenção, enquanto o Marco Civil da Internet organiza os direitos e as responsabilidades no ambiente digital. Contudo, a existência desses marcos não elimina as lacunas práticas.

Confirmou-se a hipótese de que a efetividade da proteção é limitada por desafios jurídicos, tecnológicos e institucionais. Mesmo com o retorno da ação penal pública incondicionada, que retira da vítima o ônus da representação, a prova digital continua volátil; a autoria permanece fragmentada; os valores são rapidamente dissipados; os canais de atendimento são complexos; e a cooperação entre os bancos, as plataformas, a polícia, o Ministério Público, o Judiciário e os órgãos administrativos ainda é insuficiente. A vítima idosa frequentemente enfrenta uma peregrinação burocrática que agrava o dano sofrido.

O caso das fraudes vinculadas ao INSS, especialmente no contexto da Operação Sem Desconto,



mostrou a dimensão estrutural do problema. A apuração de descontos não autorizados em benefícios dos aposentados e dos pensionistas evidencia que a vulnerabilidade do idoso pode ser explorada não apenas por mensagens falsas, mas também por sistemas institucionais mal fiscalizados. O caso reforça a necessidade de uma governança, de uma validação robusta do consentimento, de bloqueios cautelares e de mecanismos coletivos de ressarcimento.

Conclui-se que o enfrentamento ao estelionato digital contra os idosos exige uma resposta integrada. No plano legislativo, a Lei nº 15.397/2026 preencheu lacunas importantes ao criminalizar a logística das "contas-laranja", mas ainda são necessários protocolos reforçados para as contratações digitais e os descontos que envolvem os idosos. No plano institucional, é indispensável fortalecer as delegacias, os canais bancários prioritários, a cooperação interinstitucional e a atuação preventiva dos órgãos de controle. No plano tecnológico, deve-se adotar uma autenticação acessível, o monitoramento de operações suspeitas e as trilhas auditáveis. No plano social, a educação digital permanente é uma medida essencial.

A proteção da pessoa idosa no ambiente digital deve ser compreendida como uma expressão concreta da dignidade humana. O objetivo não é afastar os idosos da tecnologia, mas garantir que possam utilizá-la com segurança, com autonomia e com confiança. Uma sociedade que digitaliza os serviços essenciais sem proteger seus grupos vulneráveis transforma a inovação em um risco. Por isso, a efetivação dos direitos das vítimas idosas exige que o Direito acompanhe a tecnologia sem abandonar sua finalidade maior: proteger a pessoa humana contra novas formas de injustiça.

REFERÊNCIAS

AGÊNCIA BRASIL. **Golpes pela internet aumentam contra população idosa**. Rádioagência Nacional, Brasília, DF, 15 jun. 2024. Disponível em: <https://agenciabrasil.ebc.com.br/radioagencia-nacional/direitos-humanos/audio/2024-06/golpes-pela-internet-aumentam-contrapopulacao-idosa>. Acesso em: 1 jun. 2026.

BARATTA, Alessandro. **Criminologia crítica e crítica do Direito Penal**. 11. ed. Rio de Janeiro: Revan, 2020.

BARROSO, Luís Roberto. **Curso de direito constitucional contemporâneo: os conceitos fundamentais e a construção do novo modelo**. 6. ed. São Paulo: Saraiva, 2017.

BOTTINI, Pierpaolo. **Crimes digitais e proteção penal**. São Paulo: Revista dos Tribunais, 2023.

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: 1 jun. 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: 1 jun. 2026.



BRASIL. **Decreto-Lei nº 3.689, de 3 de outubro de 1941.** Código de Processo Penal. Brasília, DF: Presidência da República, 1941. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 1 jun. 2026.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990.** Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: Presidência da República, 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/18078compilado.htm. Acesso em: 1 jun. 2026.

BRASIL. **Lei nº 9.613, de 3 de março de 1998.** Dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; cria o Conselho de Controle de Atividades Financeiras - COAF. Brasília, DF: Presidência da República, 1998. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/19613compilado.htm. Acesso em: 02 jun. 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: http://www.planalto.gov.br/ccivil_03/leis/2003/110.741.htm. Acesso em: 1 jun. 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: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm. Acesso em: 1 jun. 2026.

BRASIL. **Lei nº 13.105, de 16 de março de 2015.** Código de Processo Civil. Brasília, DF: Presidência da República, 2015. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/113105.htm. Acesso em: 1 jun. 2026.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em: 1 jun. 2026.

BRASIL. **Lei nº 14.155, de 27 de maio de 2021.** Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet. Brasília, DF: Presidência da República, 2021. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/114155.htm. Acesso em: 1 jun. 2026.

BRASIL. **Lei nº 14.478, de 21 de dezembro de 2022.** Dispõe sobre diretrizes a serem observadas na prestação de serviços de ativos virtuais e na regulamentação das prestadoras de serviços de ativos virtuais. Brasília, DF: Presidência da República, 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/114155.htm. Acesso em: 1 jun. 2026.

BRASIL. **Lei nº 15.397, de 30 de abril de 2026.** Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), a fim de majorar as penas previstas para os crimes de furto, roubo, estelionato, receptação, receptação de animal e interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública, bem como para tipificar os crimes de receptação de animal doméstico e de fraude bancária. Brasília, DF: Presidência da República, 2026. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/lei/115397.htm. Acesso em: 02 jun. 2026.



BRASIL. Advocacia-Geral da União. **AGU obtém bloqueio de mais R\$ 500 milhões para ressarcir aposentados e pensionistas**. Brasília, DF, 17 dez. 2025. Disponível em: <https://www.gov.br/agu/pt-br/comunicacao/noticias/agu-obtem-bloqueio-de-mais-r-500-milhoes-para-ressarcir-aposentados-e-pensionistas>. Acesso em: 1 jun. 2026.

BRASIL. Controladoria-Geral da União. **Operação combate descontos não autorizados de aposentados e pensionistas; valor pode chegar a R\$ 6,3 bi**. Brasília, DF, 23 abr. 2025. Disponível em: <https://www.gov.br/cgu/pt-br/assuntos/noticias/2025/04/fraude-no-inss-aposentados-e-pensionistas-tiveram-quase-r-6-3-bi-em-descontos-sem-autorizacao>. Acesso em: 1 jun. 2026.

BRASIL. Instituto Nacional do Seguro Social. **É golpe! INSS não vai à casa dos segurados para pedir dados**. Brasília, DF, 22 abr. 2026. Disponível em: <https://www.gov.br/inss/pt-br/assuntos/e-golpe-inss-nao-vai-a-casa-dos-segurados-para-pedir-dados>. Acesso em: 1 jun. 2026.

BRASIL. Superior Tribunal de Justiça. **Súmula nº 297**. O Código de Defesa do Consumidor é aplicável às instituições financeiras. Segunda Seção, julgada em 12 maio 2004. **Diário da Justiça**, Brasília, DF, 9 set. 2004, p. 149. Disponível em: <https://scon.stj.jus.br/SCON/sumstj>. Acesso em: 1 jun. 2026.

CAMARANO, Ana Amélia. **Envelhecimento e vulnerabilidade no Brasil**. Rio de Janeiro: IPEA, 2022.

CARVALHO DIAS, Ronaldo Bretas. **Direitos da pessoa idosa: proteção, garantias e desafios**. Belo Horizonte: D'Plácido, 2022.

CASTELLS, Manuel. **A sociedade em rede**. São Paulo: Paz e Terra, 2020.

CAVALIERI FILHO, Sérgio. **Programa de responsabilidade civil**. 15. ed. São Paulo: Atlas, 2021.

CERT.br. **Phishing e outros golpes**. In: Cartilha de segurança para internet. São Paulo: Comitê Gestor da Internet no Brasil, 2023. Disponível em: <https://cartilha.cert.br/>. Acesso em: 1 jun. 2026.

DEBERT, Guita. **Envelhecimento e novas tecnologias: desafios contemporâneos**. São Paulo: Unesp, 2023.

DESSAUNE, Marcos. **Teoria aprofundada do desvio produtivo do consumidor: o prejuízo do tempo desperdiçado e da vida alterada**. 3. ed. Vitória: Edição do Autor, 2022.

DIDIER JR., Fredie et al. **Curso de direito processual civil**. Salvador: JusPodivm, 2021.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. São Paulo: Atlas, 2020.

DONEDA, Danilo; WIMMER, Miriam. **Regulação de dados pessoais no Brasil**. Rio de Janeiro: Forense, 2021.

LIMA, Katia S. P. **Crimes digitais: desafios e tendências**. São Paulo: Saraiva, 2023.

MARQUES, Cláudia Lima; BENJAMIN, Antônio Herman; MIRAGEM, Bruno. **Comentários ao Código de Defesa do Consumidor**. 7. ed. São Paulo: Revista dos Tribunais, 2021.

MIRAGEM, Bruno. **Curso de direito do consumidor**. 9. ed. São Paulo: Revista dos Tribunais, 2022.



- MORAES, Alexandre de. **Direitos humanos fundamentais**. 12. ed. São Paulo: Atlas, 2019.
- MOTA ALVES, Fabrício da. **Investigação e prova digital no Brasil**. São Paulo: Atlas, 2022.
- NERI, Anita Liberalesso. **Psicologia do envelhecimento**. Campinas: Alínea, 2020.
- NUCCI, Guilherme de Souza. **Manual de processo penal**. São Paulo: Forense, 2022.
- ORGANIZAÇÃO DOS ESTADOS AMERICANOS. **Convenção Interamericana sobre a Proteção dos Direitos Humanos dos Idosos**. Washington, D.C., 2015.
- PECK, Patrícia. **Direito digital brasileiro**. 6. ed. São Paulo: Saraiva, 2022.
- RIBEIRO, Oscar; PAÚL, Constança. **O envelhecimento e os direitos humanos**. Porto: UPorto Press, 2019.
- SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais**. 12. ed. Porto Alegre: Livraria do Advogado, 2012.
- SCHREIBER, Anderson. **Tratamento de dados pessoais e proteção jurídica**. Rio de Janeiro: Forense, 2021.
- _____. **Proteção de dados pessoais e direitos fundamentais**. Rio de Janeiro: Forense, 2021.
- VAINZOF, Rony. **Cibersegurança e crimes informáticos**. São Paulo: Thomson Reuters, 2021.
- VERAS, Renato. **Envelhecimento saudável: desafios atuais**. Rio de Janeiro: Fiocruz, 2021.