Revista ARACÊ
ISSN: 2358-2472

ASPECTOS PENAIS DO ESTELIONATO E FALSIDADE IDEOLÓGICA EM MARKETPLACES DIGITAIS

CRIMINAL ASPECTS OF FRAUD AND IDEOLOGICAL FALSEHOOD IN DIGITAL MARKETPLACES

ASPECTOS PENALES DE LA ESTAFA Y DE LA FALSEDAD IDEOLÓGICA EN LOS MARKETPLACES DIGITALES

https://doi.org/10.56238/arev8n5-082

Data de submissão: 20/04/2026 **Data de publicação:** 20/05/2026

Irene Pereira Sottoriva
Bacharelando em Direito
Instituição: Faculdades Integradas Aparício Carvalho (FIMCA/JARU)
Endereço: Rondônia, Brasil
E-mail: sottorivairenepr@gmail.com

Marcos Chianesi Júnior
Bacharelando em Direito
Instituição: Faculdades Integradas Aparício Carvalho (FIMCA/JARU)
Endereço: Rondônia, Brasil
E-mail: marcoschiane@gmail.com

RESUMO

O artigo investiga como o Direito Penal brasileiro responde às fraudes praticadas em marketplaces digitais, especialmente no que se refere à aplicação dos arts. 171, 299 e 307 do Código Penal. A análise demonstra que o estelionato eletrônico ocupa posição central nesse contexto, mas que a identificação de falsidade ideológica ou de falsa identidade depende das características concretas da conduta e do suporte utilizado para a fraude. Também são abordados temas como prova digital, cadeia de custódia, competência, consunção e os limites da atuação das plataformas diante de práticas ilícitas cometidas por terceiros. A pesquisa evidencia a necessidade de maior precisão na qualificação jurídica dos fatos e de cautela na apreciação da prova produzida em ambiente digital.

Palavras-chave: Estelionato Eletrônico. Falsidade Ideológica. Falsa Identidade. Marketplaces Digitais. Prova Digital.

ABSTRACT

This article investigates how Brazilian criminal law responds to fraud committed on digital marketplaces, especially regarding the application of Articles 171, 299 and 307 of the Brazilian Penal Code. The analysis shows that electronic fraud plays a central role in this context, but the identification of ideological falsehood or false identity depends on the specific features of the conduct and on the means used to carry out the fraud. It also addresses issues such as digital evidence, chain of custody, jurisdiction, absorption of offenses, and the limits of platform action in relation to unlawful practices committed by third parties. The research highlights the need for greater precision in the legal classification of facts and for caution in the assessment of evidence produced in digital environments.

Revista ARACÊ
ISSN: 2358-2472

Keywords: Electronic Fraud. Ideological Falsehood. False Identity. Digital Marketplaces. Digital Evidence.

RESUMEN
El artículo investiga cómo el Derecho Penal brasileño responde a los fraudes cometidos en marketplaces digitales, especialmente en lo que respecta a la aplicación de los artículos 171, 299 y 307 del Código Penal. El análisis demuestra que la estafa electrónica ocupa una posición central en este contexto, pero que la identificación de la falsedad ideológica o de la falsa identidad depende de las características concretas de la conducta y del medio utilizado para perpetrar el fraude. También se abordan temas como la prueba digital, la cadena de custodia, la competencia, la consunción y los límites de la actuación de las plataformas frente a prácticas ilícitas cometidas por terceros. La investigación pone de manifiesto la necesidad de una mayor precisión en la calificación jurídica de los hechos y de cautela en la valoración de la prueba producida en el entorno digital.

Palabras clave: Estafa Electrónica. Falsedad Ideológica. Falsa Identidad. Marketplaces Digitales. Prueba Digital.

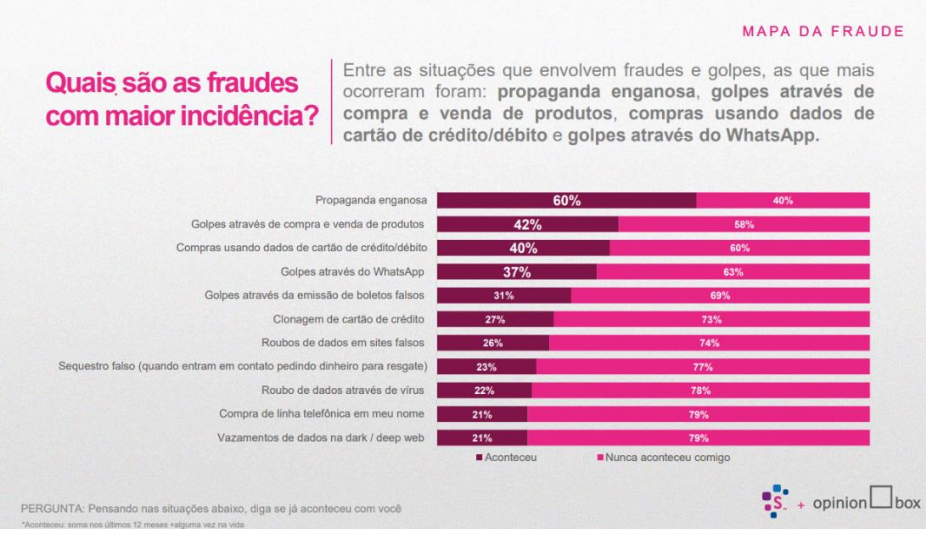
Revista ARACÊ
ISSN: 2358-2472

1 INTRODUÇÃO

A consolidação dos marketplaces digitais como infraestrutura ordinária de circulação de bens e serviços modificou a forma de contratar, pagar e confiar. Em um mesmo ambiente virtual, podem coexistir classificados eletrônicos, intermediação negocial, sistemas reputacionais, chats internos, meios integrados de pagamento, logística e mecanismos de autenticação. Essa arquitetura ampliou a eficiência econômica, mas também multiplicou as oportunidades de fraude patrimonial, sobretudo quando o agente desloca a vítima para canais externos, manipula a aparência de legitimidade da plataforma, utiliza dados cadastrais inexatos ou faz circular comprovantes eletrônicos falsos.

Os indicadores institucionais confirmam a relevância do problema. A Serasa Experian registrou 3.468.255 tentativas de fraude no primeiro trimestre de 2025, com crescimento de 22,9% em relação ao mesmo período de 2024, e 6.937.832 tentativas no primeiro semestre de 2025. Em paralelo, o Fórum Brasileiro de Segurança Pública apontou 2.166.552 registros de estelionato em 2024, com crescimento de 7,8% em relação ao ano anterior, evidenciando a progressiva migração da criminalidade patrimonial para o ambiente digital (SERASA EXPERIAN, 2025a; SERASA EXPERIAN, 2025b; FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA, 2025).

Figura 1. Mapa da fraude



Fonte: Serasa Experian (2021).

Do ponto de vista penal, o problema exige análise técnica e não pode ser resolvido por automatismos. O art. 171 do Código Penal permanece como eixo típico das fraudes patrimoniais praticadas por meio eletrônico, especialmente após a Lei nº 14.155/2021. Já o art. 299 exige declaração falsa ou omissão em documento público ou particular com aptidão para prejudicar direito, criar obrigação ou alterar a verdade sobre fato juridicamente relevante. Em paralelo, o art. 307 tutela a fé

Revista ARACÊ
ISSN: 2358-2472

pública na individuação pessoal, tendo o STJ consolidado, no Tema 1.255, que a falsa identidade é crime formal, consumado com o fornecimento consciente e voluntário de dados inexatos sobre a real identidade, independentemente de vantagem ou dano concreto (BRASIL, 1940; BRASIL, 2021; SUPERIOR TRIBUNAL DE JUSTIÇA, 2025a).

A questão central deste artigo consiste em verificar em que medida as fraudes praticadas em marketplaces digitais configuram estelionato eletrônico e em quais hipóteses a falsidade ideológica efetivamente se caracteriza, sem confusão com a falsa identidade ou com outras falsidades documentais. Também se examina como a prova digital deve ser preservada, quais obstáculos processuais persistem e em que medida a discussão sobre plataformas pertence ao campo penal ou, predominantemente, ao campo civil-regulatório.

Parte-se da hipótese de que o art. 171 do Código Penal, especialmente após a Lei nº 14.155/2021, constitui o núcleo típico predominante nas fraudes de marketplace; que a falsidade ideológica depende de suporte documental juridicamente relevante; que a falsa identidade exige análise autônoma; e que a responsabilização das plataformas, em regra, apresenta maior densidade no plano civil e regulatório, sem autorização para imputação penal automática por omissão.

O objetivo deste artigo é analisar, à luz da legislação penal e processual, da jurisprudência e dos dados institucionais disponíveis, os critérios de distinção entre estelionato eletrônico, falsa identidade, falsidade ideológica, uso de documento falso e consunção nas fraudes praticadas em marketplaces digitais, bem como examinar os limites jurídicos da responsabilização das plataformas e os requisitos de validade da prova digital.

1.1 MARKETPLACES E O RELEVO JURÍDICO-PENAL DO PROBLEMA

O vocábulo “marketplace” não recebe definição fechada no ordenamento brasileiro, mas pode ser compreendido, para fins deste estudo, como o ambiente digital que aproxima usuários para publicação de anúncios e realização de operações de compra e venda, podendo a plataforma limitar-se à aproximação das partes ou assumir funções adicionais de pagamento, reputação, moderação, logística e resolução de disputas. Essa diferença não é apenas empresarial; ela influencia diretamente o regime jurídico aplicável, a extensão do dever de segurança, a disponibilidade de vestígios digitais e a própria análise do nexo causal nas fraudes.

Do ponto de vista normativo, os marketplaces podem ser compreendidos, em termos gerais, como aplicações de internet submetidas ao Marco Civil da Internet, sem prejuízo da incidência do Código de Defesa do Consumidor quando configurada cadeia de fornecimento. A depender do desenho do serviço, o provedor pode aproximar-se do modelo de simples classificado digital ou, ao

Revista ARACÊ
ISSN: 2358-2472

contrário, assumir posição mais intensa de intermediador, com mecanismos próprios de autenticação, reputação, pagamento e gestão do risco. Essa distinção aparece tanto na doutrina quanto na jurisprudência e é decisiva para o tratamento das fraudes (BRASIL, 2014; BRASIL, 1990; BRITO, 2023).

Em precedente paradigmático, o Superior Tribunal de Justiça concluiu que o intermediador não responde quando a fraude se desenvolve fora da plataforma e sem o uso dos mecanismos disponibilizados ao usuário, por entender rompido o nexo causal entre a prestação do serviço e o dano experimentado pela vítima. A orientação é relevante para o presente estudo porque demonstra que, mesmo em ambientes digitais de intermediação, a responsabilização jurídica depende do modo concreto de execução do golpe e do grau de vinculação entre a arquitetura da plataforma e o resultado lesivo.

Nesse sentido, o (REsp nº 1.880.344/SP) reforça que a simples existência do ambiente eletrônico não basta, por si só, para atrair responsabilidade do intermediador:

> CIVIL. RECURSO ESPECIAL. AÇÃO DE COMPENSAÇÃO DE DANOS MATERIAIS. VIOLAÇÃO A DISPOSITIVO DA CF. NÃO CONHECIMENTO. FRAUDE PRATICADA POR ADQUIRENTE DE PRODUTO ANUNCIADO NO MERCADO LIVRE. ENDEREÇO DE E-MAIL FALSO. PRODUTO ENTREGE SEM O RECEBIMENTO DA CONTRAPRESTAÇÃO EXIGIDA. FALHA NA PRESTAÇÃO DOS SERVIÇOS. INEXISTÊNCIA. FATO DE TERCEIRO. ROMPIMENTO DO NEXO DE CAUSALIDADE. JULGAMENTO: CPC/2015 - RECURSO ESPECIAL Nº 1.880.344 - SP (2020/0149326-1).

Nos marketplaces, a fraude costuma assumir formas repetidas: anúncio falso de produto inexistente; golpe do falso comprador com comprovante manipulado; golpe do intermediário; desvio da conversa para WhatsApp ou e-mail; criação de conta recebedora com dados inexatos; “reativação” fraudulenta de compra cancelada; utilização de boletos, QR Codes e comprovantes adulterados; e simulação de procedimentos internos da própria plataforma. A recorrência dessas práticas demonstra que a mentira sobre identidade, pagamento ou titularidade raramente aparece de forma isolada: ela integra uma engenharia social destinada à obtenção de vantagem patrimonial ilícita.

Essa constatação recomenda um método analítico preciso. A tipificação deve partir do núcleo patrimonial do fato, o induzimento ou manutenção da vítima em erro para obtenção de vantagem ilícita, e só depois examinar se a identidade simulada, o cadastro inexato ou o documento falsificado possuem autonomia ofensiva suficiente para justificar imputação adicional. O caminho inverso, que parte do “falso” para depois procurar prejuízo patrimonial, produz com frequência exagero punitivo, duplicidade valorativa e enquadramentos inadequados.

Revista ARACÊ
ISSN: 2358-2472

2 REFERENCIAL TEÓRICO

O art. 171 do Código Penal tipifica a obtenção, para si ou para outrem, de vantagem ilícita em prejuízo alheio, induzindo ou mantendo alguém em erro mediante artifício, ardil ou qualquer outro meio fraudulento. A redação básica do tipo já era suficientemente ampla para alcançar fraudes patrimoniais praticadas em ambiente digital; a Lei nº 14.155/2021, contudo, reforçou a tutela penal ao prever forma qualificada quando a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos, correio eletrônico fraudulento ou meio análogo, com pena de reclusão de quatro a oito anos e multa (BRASIL, 1940; BRASIL, 2021).

A importância dessa alteração legislativa é dupla. Em primeiro lugar, evidencia que o chamado estelionato eletrônico não se restringe ao furto silencioso de credenciais bancárias: inclui engenharia social, construção de perfis falsos, manipulação do ambiente de confiança e deslocamento comunicacional para canais paralelos. Em segundo lugar, o diploma de 2021 também repercutiu na competência processual, ao alterar o § 4º do art. 70 do Código de Processo Penal para hipóteses específicas envolvendo depósito, transferência, emissão de cheque sem provisão ou frustração de pagamento. O STJ enfatizou, todavia, que a reforma não universalizou o domicílio da vítima como foro de toda e qualquer fraude digital, mas apenas para as situações descritas pelo legislador (SUPERIOR TRIBUNAL DE JUSTIÇA, 2022).

No plano prático, o estelionato em marketplaces digitais costuma apresentar cadeias executivas heterogêneas. Há casos em que a fraude se consuma com o pagamento antecipado de mercadoria inexistente; em outros, o agente obtém a posse da coisa mediante exibição de comprovante inexistente ou adulterado; em outros ainda, o golpe se realiza na fase de "liberação" da venda, quando a vítima é convencida a pagar taxa, seguro, frete ou valor de reativação. Em todas essas hipóteses, o eixo normativo principal continua sendo o art. 171, porque o núcleo do comportamento é patrimonial e pressupõe vantagem ilícita obtida por meio enganoso.

A disciplina da ação penal do estelionato também sofreu mutações recentes. Após a reforma promovida pela Lei nº 13.964/2019, consolidou-se, em diversas hipóteses, a necessidade de representação da vítima, mas o legislador continuou ajustando o regime para grupos vulneráveis. Em 2025, a Lei nº 15.229 alterou o § 5º do art. 171 para estabelecer ação penal pública incondicionada quando o estelionato é cometido contra pessoa com deficiência. O dado não altera o núcleo do presente estudo, mas demonstra que a tutela penal do patrimônio permanece em atualização normativa, sobretudo em ambientes de maior vulnerabilidade digital (BRASIL, 2019; BRASIL, 2025).

A leitura dogmática adequada do estelionato eletrônico em marketplaces exige, portanto, duas

Revista ARACÊ
ISSN: 2358-2472

cautelas. A primeira é evitar restringir o tipo a fraudes bancárias clássicas, desconsiderando a sofisticação da engenharia social contemporânea. A segunda é não permitir que a modernização legislativa dissolva exigências estruturais do delito: vantagem ilícita, prejuízo alheio, erro da vítima e emprego de meio fraudulento continuam sendo elementos centrais e devem ser demonstrados de forma concreta.

2.1 FALSIDADE IDEOLÓGICA, FALSA IDENTIDADE E DOCUMENTOS ELETRÔNICOS

Se o estelionato é, em regra, o tipo principal nas fraudes de marketplace, a falsidade ideológica só ingressa em cena quando o agente omite, em documento público ou particular, declaração que dele devia constar, ou nele faz inserir ou inserir declaração falsa ou diversa da que devia ser escrita, com o fim de prejudicar direito, criar obrigação ou alterar a verdade sobre fato juridicamente relevante. O núcleo do art. 299 do Código Penal é documental. Por isso, a mera existência de perfil falso, apelido, nome de fantasia ou fotografia enganosa em ambiente informal de negociação não basta, por si só, para caracterizar falsidade ideológica. É necessário demonstrar a presença de um suporte documental qualificado e a aptidão da declaração para atingir a fé pública ou interesse juridicamente protegido nessa dimensão (BRASIL, 1940).

Em ambiente digital, o art. 299 pode ser cogitado quando a fraude envolve cadastro eletrônico dotado de relevo jurídico-documental, formulário contratual, comprovante ideologicamente falso, declaração inserida em instrumento particular eletrônico ou documentação criada para alterar a verdade sobre identidade, titularidade, pagamento ou existência da obrigação. O ponto decisivo é funcional: o documento digital permanece sendo documento para fins penais, mas não qualquer manifestação eletrônica informal se converte, automaticamente, em documento penalmente relevante.

Diversa é a situação do art. 307 do Código Penal. Em 2025, ao julgar o Tema Repetitivo 1.255, o STJ fixou a tese de que o delito de falsa identidade é crime formal e se consuma quando o agente fornece, consciente e voluntariamente, dados inexatos sobre sua real identidade, independentemente da ocorrência de resultado naturalístico. A orientação é central para as fraudes em marketplaces, porque muitos golpes começam justamente com a personificação fraudulenta do agente, seja para inspirar confiança, seja para viabilizar abertura de conta, aproximação da vítima ou recebimento de valores (SUPERIOR TRIBUNAL DE JUSTIÇA, 2025a).

Também pode surgir, em certas fraudes de marketplace, o debate sobre uso de documento falso, especialmente quando o agente encaminha comprovante de pagamento, identidade, comprovante de residência, procuração, recibo ou contrato adulterado para persuadir a vítima ou a instituição financeira. Nesses casos, a distinção entre documento materialmente falso, documento

Revista ARACÊ
ISSN: 2358-2472

ideologicamente falso e mera mensagem enganosa é decisiva. A depender da estrutura do artefato e de sua circulação, pode haver espaço para os arts. 298 e 304 do Código Penal; porém, novamente, o intérprete deve verificar se o documento possui autonomia ofensiva ou se constitui simples meio de indução ao erro patrimonial.

O precedente repetitivo do STJ impede o raciocínio simplista segundo o qual toda mentira sobre a própria identidade seria irrelevante até que se comprove prejuízo patrimonial ou documento ideologicamente falso. Ao mesmo tempo, o mesmo precedente não autoriza a multiplicação acrítica de imputações. Se o agente apenas se atribui identidade falsa perante a vítima, sem inserir declaração em documento relevante, o art. 307 tende a ser, em tese, mais adequado do que o art. 299. Se, além disso, produz documento materialmente falso ou faz circular comprovante alterado, podem surgir outros tipos documentais. E se o falso serve unicamente como etapa de consumação do estelionato, reaparece a discussão sobre consunção.

Nesse ponto, a Súmula 17 do STJ conserva plena utilidade: quando o falso se exaure no estelionato, sem mais potencialidade lesiva, é por este absorvido. O enunciado não elimina o falso em abstrato; apenas impede dupla valoração quando a falsidade funciona como meio normal, desprovido de autonomia lesiva, para a fraude patrimonial. Em marketplaces, isso ocorre com frequência em comprovantes, e-mails e documentos cuja única função é enganar a vítima para liberar o bem ou efetuar novo pagamento. Já quando o documento falso possui circulação própria, capacidade de enganar terceiros para além da vítima imediata ou afeta interesse distinto, a autonomia típica pode subsistir (SUPERIOR TRIBUNAL DE JUSTIÇA, 1990).

Para tornar operacional essa distinção, propõe-se um teste dogmático em seis etapas: identificar o núcleo patrimonial do fato; verificar se houve autêntica personificação enganosa do agente; definir se o suporte utilizado possui natureza documental relevante; examinar se o falso possui autonomia ofensiva; averiguar se houve efetivo uso ou mera preparação; e, por fim, testar a incidência da consunção. Esse itinerário interpretativo reduz o risco de enquadrar todo perfil falso como falsidade ideológica, preserva a coerência sistemática entre os arts. 171, 299, 307, 298 e 304 do Código Penal e oferece maior segurança para a persecução penal e para a defesa.

Revista ARACÊ
ISSN: 2358-2472

Quadro 1. Critérios mínimos de enquadramento penal em fraudes de marketplace.

Conduta predominante	Tipo penal em tese	Requisito distintivo	Observação analítica
Induzir a vítima em erro para obter pagamento, envio de produto ou liberação de serviço	Art. 171 do CP, inclusive § 2º-A quando presentes os meios eletrônicos da Lei nº 14.155/2021	Vantagem ilícita, prejuízo alheio e meio fraudulento	Núcleo típico mais frequente nas fraudes patrimoniais em marketplaces
Atribuir-se identidade falsa para inspirar confiança ou ocultar a real identidade	Art. 307 do CP	Fornecimento consciente e voluntário de dados inexatos sobre a própria identidade	Crime formal segundo o Tema Repetitivo 1.255 do STJ
Inserir declaração falsa em cadastro, instrumento ou comprovante com relevância documental	Art. 299 do CP	Documento público ou particular e alteração da verdade sobre fato juridicamente relevante	Nem todo perfil falso ou nickname configura falsidade ideológica
Utilizar comprovante ou documento materialmente/ideologicamente falso com circulação autônoma	Arts. 298, 299 ou 304 do CP, conforme o caso	Autonomia lesiva do documento e efetiva circulação/uso	Exige exame concreto do suporte, da autoria e da potencialidade ofensiva
Emprego do falso apenas como meio normal para consumar o golpe patrimonial	Absorção pelo estelionato (Súmula 17 do STJ)	Ausência de potencialidade lesiva autônoma do falso	Evita bis in idem e qualificação excessiva dos fatos

Fonte: Elaboração própria, com base em BRASIL (1940; 2021) e SUPERIOR TRIBUNAL DE JUSTIÇA (1990; 2025a).

2.2 PROVA DIGITAL, CADEIA DE CUSTÓDIA E CONFIABILIDADE

A qualificação típica adequada não resolve, por si só, o problema da efetividade da tutela penal. Em fraudes digitais, a dificuldade mais recorrente está na preservação, identificação e valoração dos vestígios eletrônicos. O art. 158-A do Código de Processo Penal define cadeia de custódia como o conjunto de procedimentos destinado a manter e documentar a história cronológica do vestígio coletado, de modo a rastrear sua posse e manuseio desde o reconhecimento até o descarte. Embora o dispositivo tenha sido concebido de maneira geral, ele oferece parâmetro indispensável para a prova digital, cuja volatilidade, replicabilidade e suscetibilidade à manipulação exigem cautelas acrescidas (BRASIL, 1941).

A literatura contemporânea é enfática ao sustentar que as provas digitais demandam disciplina jurídica própria. Saad, Rossi e Partata demonstram que a obtenção, preservação e valoração desse tipo de vestígio não podem ser regidas por mera transposição automática das categorias analógicas, pois os dados eletrônicos dependem de metadados, registram múltiplas camadas de contexto, circulam por ambientes distribuídos e podem ser alterados com extrema facilidade. No mesmo sentido, Araújo destaca que tecnologias como blockchain, trilhas de auditoria e mecanismos de integridade podem contribuir para uma cadeia de custódia mais robusta, desde que não se confunda inovação tecnológica

Revista ARACÊ
ISSN: 2358-2472

com dispensa de garantias processuais (SAAD; ROSSI; PARTATA, 2024; ARAÚJO, 2024).

O Superior Tribunal de Justiça também vem reforçando a centralidade da integridade metodológica. Em 2024, a Quinta Turma não admitiu como prova prints extraídos de aparelho celular sem metodologia apta a demonstrar autenticidade, completude e confiabilidade dos dados. A orientação não significa que a captura de tela seja sempre inútil; significa, isto sim, que ela deve ser contextualizada, documentada e, quando necessário, complementada por extração técnica, perícia, preservação do arquivo original e correlação com outras fontes de prova (SUPERIOR TRIBUNAL DE JUSTIÇA, 2024a).

Nos golpes de marketplace, a prova costuma envolver anúncio, conversas, comprovantes, dados bancários, URL, logs, IPs, registros das plataformas e relatórios antifraude. A confiabilidade desses elementos depende da preservação contextual, da indicação da origem, do método de extração e da possibilidade de verificação de integridade.

É igualmente importante lembrar que o ordenamento brasileiro já dispõe de instrumentos úteis para estabilização de prova digital, ainda que produzidos em ramos processuais diversos. O art. 384 do Código de Processo Civil admite a ata notarial para atestar a existência e o modo de existir de fato, inclusive com arquivos eletrônicos, imagens e sons. Embora a ata notarial não substitua a cadeia de custódia penal nem a perícia quando necessária, ela pode contribuir para fixar o estado de um anúncio, a aparência de um diálogo ou a existência de determinado conteúdo em momento específico, reduzindo o risco de desaparecimento do vestígio (BRASIL, 2015).

Em termos institucionais, o CNJ passou a dedicar atenção específica à coleta e à preservação de provas digitais no processo penal. O seminário promovido em 2025 reforçou a necessidade de boas práticas, interoperabilidade entre atores públicos e privados e desenvolvimento de rotinas de rastreabilidade compatíveis com a realidade contemporânea. Em outras palavras, o problema da fraude em marketplaces não é apenas dogmático; é também de governança probatória (CONSELHO NACIONAL DE JUSTIÇA, 2025a; CONSELHO NACIONAL DE JUSTIÇA, 2025b).

2.3 LIMITES DA RESPONSABILIDADE DAS PLATAFORMAS DIGITAIS

A discussão sobre plataformas digitais ganhou densidade institucional recente. Em 2024, a Advocacia-Geral da União defendeu, perante o Supremo Tribunal Federal, a ampliação das responsabilidades civis das plataformas por conteúdo ilícito de terceiros, sustentando maior proatividade na moderação e admitindo responsabilização civil em hipóteses de omissão após notificação, como invasão de perfis ou criação de contas fraudulentas em nome de terceiros. Em 2025, o STF definiu parâmetros para a responsabilização de plataformas por conteúdos de terceiros,

Revista ARACÊ
ISSN: 2358-2472

tensionando a leitura tradicional do art. 19 do Marco Civil da Internet (ADVOCACIA-GERAL DA UNIÃO, 2024; SUPREMO TRIBUNAL FEDERAL, 2025).

Esses desenvolvimentos são relevantes para o tema do presente trabalho, mas devem ser corretamente posicionados. O debate travado no STF e pela AGU é, primordialmente, de responsabilidade civil e de regulação do ambiente digital. Ele não equivale a uma autorização para afirmar que plataformas de marketplace respondem penalmente, por omissão, sempre que deixam de evitar golpes praticados por terceiros. No Direito Penal brasileiro, a responsabilidade por omissão depende de dever jurídico de agir, posição de garantidor e nexo entre a omissão e o resultado, nos termos do art. 13, § 2º, do Código Penal. A mera insuficiência de moderação, a deficiência de compliance ou a existência de falhas sistêmicas podem gerar deveres civis, administrativos e regulatórios sem, automaticamente, converter o intermediário em autor ou partícipe penal do estelionato praticado por usuário da plataforma (BRASIL, 1940).

Isso não significa irrelevância jurídica das plataformas. Ao contrário, a prevenção de golpes em marketplaces exige políticas robustas de identificação e verificação do usuário, antifraude em camadas, mecanismos de detecção de contas suspeitas, alerta ostensivo sobre desvio de negociação para aplicativos externos, preservação célere de vestígios e canais efetivos de comunicação com autoridades e consumidores. A própria Serasa Experian tem reiterado a importância da combinação entre autenticação, biometria, análise documental, inteligência de risco e educação do usuário como resposta à sofisticação da engenharia social (SERASA EXPERIAN, 2026).

Em chave de síntese, o estudo dos aspectos penais em marketplaces não prescinde da análise das plataformas, mas essa análise deve ser funcionalmente limitada. O papel da plataforma é central para a compreensão do risco, da prova e do nexo causal; todavia, sua responsabilização não se presume nem se confunde com a do fraudador. A plataforma é relevante como espaço do fato, fonte de vestígios, ator preventivo e, em certos casos, fornecedora civilmente responsável. Penalmente, contudo, a imputação exige algo qualitativamente diverso: participação dolosa, colaboração materialmente relevante ou omissão juridicamente equiparável à ação, o que deve ser demonstrado de forma rigorosa e excepcional.

3 METODOLOGIA

A pesquisa possui natureza qualitativa, com abordagem bibliográfica, documental e jurisprudencial. Foram examinados dispositivos do Código Penal, do Código de Processo Penal, do Marco Civil da Internet e do Código de Defesa do Consumidor, além de precedentes do Superior Tribunal de Justiça e do Supremo Tribunal Federal, dados institucionais sobre fraudes digitais e

Revista ARACÊ
ISSN: 2358-2472

literatura especializada sobre prova digital, cadeia de custódia e responsabilidade de plataformas. A análise foi organizada em três eixos: identificação do contexto empírico da fraude digital, sistematização das modalidades recorrentes de golpe em marketplaces e extração de consequências jurídico-penais e processuais a partir da legislação e da jurisprudência recente.

4 RESULTADOS E DISCUSSÕES

4.1 DADOS OFICIAIS DE FRAUDE DIGITAL E SUA UTILIDADE PARA O OBJETO DO ESTUDO

Os dados oficiais disponíveis não foram produzidos especificamente para marketplaces, mas oferecem uma moldura importante para compreender a escala do problema. Informações divulgadas pela Serasa Experian mostram volume expressivo de tentativas de fraude e destacam a recorrência de inconsistências cadastrais, documentos suspeitos e obstáculos na validação biométrica (SERASA EXPERIAN, 2025a; 2025b; 2025c; 2025d). Esses elementos são particularmente úteis ao objeto desta pesquisa porque revelam que o golpe digital contemporâneo dificilmente se resume a mero inadimplemento ou descumprimento contratual; em grande número de casos, ele se estrutura a partir da manipulação de identidade, cadastro e aparência documental.

Quadro 2. Indicadores oficiais de fraude digital.

Período/recorte	Dado oficial	Resultado	Relevância analítica
Ano de 2024	Tentativas de fraude registradas no Brasil	11.509.214 ocorrências; alta de 9,4% em relação ao ano anterior	Confirma a expansão estrutural da fraude digital no país.
1º trimestre de 2025	Tentativas de fraude	3.468.255 ocorrências; uma tentativa a cada 2,2 segundos	Demonstra persistência do fenômeno em patamar elevado.
1º trimestre de 2025	Modalidades detectadas	50,6% inconsistências cadastrais; 41,9% autenticidade documental e validação biométrica	Evidencia a centralidade de dados identitários e documentos nas fraudes digitais.
Jan.–maio de 2025	Golpes envolvendo biometria e documento falso	2.384.340 ocorrências; crescimento de 28,3%	Reforça a necessidade de distinguir fraude patrimonial, falsa identidade e falsidades documentais.
1º semestre de 2025	Tentativas de fraude	6.937.832 ocorrências; alta de 29,5% sobre o mesmo período de 2024	Mostra agravamento do quadro e exige resposta institucional mais sofisticada.

Fonte: Elaboração própria com base em Serasa Experian (2025a; 2025b; 2025d; 2025e).

A leitura conjunta desses indicadores permite duas conclusões preliminares. A primeira é que o problema empírico possui densidade suficiente para justificar tratamento penal e processual específico. A segunda é que a fraude patrimonial em ambiente digital costuma caminhar ao lado de

Revista ARACÊ
ISSN: 2358-2472

controvérsias identitárias e documentais, o que confirma a impropriedade de respostas penais simplistas. Em outras palavras, o patrimônio segue no centro do conflito, mas o caminho escolhido pelo ardil frequentemente passa pela persona fraudulenta, pelo cadastro manipulado e pelo documento eletrônico utilizado para inspirar confiança indevida

4.2 MODALIDADES RECORRENTES DE FRAUDE EM MARKETPLACES E ENQUADRAMENTO PENAL PREDOMINANTE

A observação de decisões judiciais, da legislação e dos dados documentais permitiu sistematizar algumas modalidades recorrentes de fraude em marketplaces. O quadro a seguir não pretende esgotar todas as hipóteses, mas organiza cenários relevantes para o debate entre estelionato eletrônico, falsidade ideológica e falsa identidade. Essa sistematização ajuda a transformar o problema abstrato em matriz analítica operacional.

Quadro 3. Modalidades recorrentes de fraude em marketplaces e enquadramento jurídico-penal.

Modalidade	Dinâmica do golpe	Enquadramento predominante	Observação dogmática
Falso vendedor	Anuncia produto inexistente ou que nunca será entregue e obtém pagamento da vítima.	Art. 171 do Código Penal, com incidência do § 2º-A quando a fraude se viabiliza pelos meios eletrônicos descritos na Lei nº 14.155/2021.	A fraude patrimonial é o centro do fato; a identidade falsa pode funcionar como meio executivo.
Falso comprador com comprovante fraudulento	Recebe a mercadoria mediante exibição de comprovante inexistente ou manipulado.	Art. 171 do Código Penal; eventual discussão adicional sobre falsidade documental depende da natureza do comprovante utilizado.	Não se deve presumir art. 299; é preciso examinar o suporte documental concreto.
Uso de nome ou dados pessoais falsos para gerar confiança	O agente se apresenta com identidade inexistente ou alheia para induzir a vítima em erro.	Art. 171, em concurso aparente ou material com o art. 307, conforme o caso.	Após o Tema 1.255 do STJ, a falsa identidade mostra-se resposta mais precisa do que a falsidade ideológica em muitas hipóteses.
Cadastro formal com documento juridicamente relevante adulterado	O agente viabiliza conta, habilitação de vendedor, recebimento ou liberação de valores com declaração falsa em documento ou cadastro relevante.	Art. 171 e possível incidência do art. 299, sem prejuízo de outras falsidades documentais.	O art. 299 só se justifica quando houver efetiva relevância jurídica da declaração inserida no documento.
Tomada indevida de conta legítima	O fraudador sequestra conta de terceiro e utiliza reputação preexistente para aplicar o golpe.	Art. 171; podem surgir delitos correlatos, como invasão de dispositivo, conforme a dinâmica fática.	A análise exige descrição técnica do acesso indevido e da cadeia de obtenção da prova.

Fonte: Elaboração própria com base em Brasil (1940; 2021) e Superior Tribunal de Justiça (2025a).

Revista ARACÊ
ISSN: 2358-2472

O quadro demonstra que o título do trabalho pode ser preservado com correção técnica desde que a falsidade ideológica seja tratada como hipótese qualificada, e não como reflexo automático de qualquer conta ou perfil falso. A pergunta decisiva deixa de ser se houve mentira em ambiente digital e passa a ser se a declaração inverídica ingressou em documento apto a produzir efeitos jurídicos concretos. Quando a resposta é negativa, a tendência é que a fraude permaneça concentrada no estelionato e, em determinadas situações, na falsa identidade. Quando positiva, abre-se espaço para o exame do art. 299, desde que o suporte documental e sua relevância sejam demonstrados com rigor. Essa distinção melhora a qualidade da imputação e reduz o risco de expansão punitiva sem lastro técnico.

4.3 MATRIZ JURISPRUDENCIAL E CONSEQUÊNCIAS PARA O TEMA

O levantamento jurisprudencial e institucional realizado para este artigo permite condensar alguns precedentes e marcos decisórios que reorientam a análise do tema. A matriz abaixo demonstra como a jurisprudência recente reorganiza o espaço dogmático entre estelionato, falsa identidade, prova digital, competência e papel das plataformas. O resultado mais importante é a substituição de respostas simplistas por critérios de diferenciação mais objetivos.

Quadro 4. Precedentes e marcos institucionais relevantes para o tema.

Fonte	Tese ou conclusão institucional	Impacto para a pesquisa
STJ, Tema 1.255 (2025)	O art. 307 do Código Penal é crime formal e se consuma com o fornecimento consciente e voluntário de dados inexatos sobre a identidade real.	Reduz o espaço para imputar falsidade ideológica em hipóteses de simples identidade simulada.
STJ, prova digital (2024)	Prints extraídos de celular sem metodologia idônea podem ser inadmissíveis.	Reforça a centralidade da cadeia de custódia em golpes de marketplace.
STJ, responsabilidade do intermediador (2021)	Não há responsabilidade do site quando a fraude ocorre fora da plataforma e sem uso de seus mecanismos.	Impede raciocínio uniforme sobre nexo causal e dever de segurança.
STJ, competência em estelionato (2022)	A Lei nº 14.155/2021 alterou a competência apenas para hipóteses específicas do art. 70, § 4º, do CPP.	Exige distinguir domicílio da vítima, local da obtenção da vantagem e modo de execução do golpe.
STF (2025)	O art. 19 do Marco Civil foi considerado parcialmente inconstitucional, com expansão da responsabilização civil das plataformas em certas hipóteses.	Atualiza o debate sobre deveres de diligência, sem autorizar responsabilização penal automática.

Fonte: Elaboração própria com base em Superior Tribunal de Justiça (2021; 2022; 2024a; 2025a) e Supremo Tribunal Federal - STF (2025)

A matriz evidencia que o direito aplicável às fraudes em marketplaces está em processo de reorganização. No plano penal, ganha força a centralidade da falsa identidade nas hipóteses de

Revista ARACÊ
ISSN: 2358-2472

simulação pessoal. No plano processual, consolida-se a compreensão de que a prova digital exige padrões mais severos de coleta e preservação. No plano civil e regulatório, o debate sobre plataformas deixa de girar apenas em torno da neutralidade do provedor e passa a incorporar deveres de prevenção e de resposta, em linha com a evolução observada na jurisprudência e nas discussões institucionais mais recentes (SUPERIOR TRIBUNAL DE JUSTIÇA, 2021a; 2022; 2024a; 2025a; SUPREMO TRIBUNAL FEDERAL, 2025). Esses três movimentos não atuam isoladamente: eles se cruzam e ajudam a explicar por que a fraude em marketplaces exige leitura integrada, sem perder a precisão própria de cada esfera jurídica.

4.4 REPERCUSSÕES PRÁTICAS PARA A PERSECUÇÃO PENAL

Em golpes de marketplace, a materialidade costuma ser fragmentada: anúncio, conversa por aplicativo, e-mail, comprovante, dado bancário, URL, histórico de acesso, denúncia formulada à plataforma e resposta automatizada do sistema. A utilidade probatória desse conjunto não decorre da mera quantidade de arquivos reunidos, mas da capacidade de demonstrar contexto, continuidade e integridade. Por isso, capturas de tela isoladas podem servir como ponto de partida da investigação, mas raramente bastam, sozinhas, para sustentar um juízo robusto de confiabilidade quando submetidas ao contraditório.

Daí decorrem quatro providências práticas relevantes: preservar o contexto do material, estabilizar o conteúdo por meios tecnicamente seguros, obter registros bancários e requisitar formalmente logs e dados cadastrais às plataformas. O processo penal perde consistência quando depende de documentos avulsos, montados sem método e apresentados sem histórico claro de obtenção. Ganha força, ao contrário, quando a cadeia de custódia é tratada desde o início como condição de confiabilidade do vestígio digital. A utilidade maior da pesquisa, nesse ponto, está em demonstrar que a qualidade da prova influencia diretamente a qualidade da imputação.

4.5 PROPOSIÇÕES PARA APERFEIÇOAMENTO JURÍDICO E INSTITUCIONAL

A primeira medida de aperfeiçoamento consiste em fortalecer deveres mínimos de identificação e rastreabilidade em aplicações de anúncios e de intermediação de compra e venda. O debate legislativo recente já revela preocupação com transparência sobre a natureza da negociação, canais de denúncia e parâmetros mínimos para identificação de usuários, como se observa no Projeto de Lei nº 4.103/2024 e nas discussões institucionais que o acompanharam no Senado Federal (SENADO FEDERAL, 2024). Ainda que tais propostas não resolvam sozinhas o problema, elas

Revista ARACÊ
ISSN: 2358-2472

mostram que o sistema jurídico começa a reagir à especificidade das fraudes praticadas em plataformas de venda.

A segunda medida passa pela adoção de políticas antifraude em camadas, combinando verificação cadastral, validação documental, monitoramento comportamental de dispositivos, detecção de duplicidade de contas e resposta rápida a relatos de irregularidade. Em marketplaces, prevenção eficaz não se resume a filtro tecnológico; envolve também desenho institucional da confiança, trilha de auditoria e possibilidade real de intervenção antes que o ardil produza dano irreversível. A própria evolução dos levantamentos recentes sobre biometria, documentos falsos e tentativas de fraude mostra que o problema exige barreiras sucessivas de contenção, e não respostas isoladas ou meramente reativas (SERASA EXPERIAN, 2025d). A adequada organização dos mecanismos de verificação tende, por isso mesmo, a reduzir não apenas a ocorrência do golpe, mas também a opacidade que costuma dificultar sua reconstrução posterior.

A terceira medida diz respeito à consolidação de protocolos mínimos de preservação de prova digital para vítimas, plataformas e autoridades. Procedimentos claros para guarda de anúncios, extração de registros, preservação contextual de mensagens e documentação do percurso do vestígio reduzem disputas futuras sobre autenticidade e fortalecem a utilidade probatória do material. Em fraudes digitais, a resposta estatal torna-se significativamente mais frágil quando o dado circula sem lastro técnico, razão pela qual a disciplina da cadeia de custódia deve deixar de ser tratada como preocupação periférica e passar a integrar a própria estratégia de enfrentamento do delito, como assinalam a doutrina processual penal especializada e os estudos voltados às provas digitais (SAAD; ROSSI; PARTATA, 2024; VAZ, 2012). Sem esse compromisso metodológico, a persecução penal permanece vulnerável justamente onde o delito mais se sofisticou: na manipulação tecnológica do vestígio.

5 CONCLUSÃO

A conclusão central é que o estelionato eletrônico permanece como eixo típico predominante das fraudes praticadas nesses ambientes. É nele que se concentra, em regra, o núcleo patrimonial do ardil, mesmo quando a execução do golpe se vale de recursos tecnológicos complexos.

Também se verificou que a falsidade ideológica não incide automaticamente. Perfil falso, nome fictício ou apresentação informal de identidade simulada não bastam, isoladamente, para preencher o art. 299 do Código Penal. A incidência desse tipo depende de declaração falsa lançada em documento juridicamente relevante. Em muitas situações, o enquadramento mais preciso se aproxima

Revista ARACÊ
ISSN: 2358-2472

da falsa identidade, justamente porque o engano é construído pela simulação da pessoa do agente e não pela falsidade ideológica documental.

No plano processual, o trabalho evidenciou que a eficácia da resposta penal está diretamente ligada à forma de preservação da prova digital. Em ambiente marcado por anúncios mutáveis, conversas instantâneas, comprovantes eletrônicos e perfis descartáveis, a cadeia de custódia deixa de ser formalidade periférica e passa a integrar o próprio mérito da discussão. Sem confiabilidade técnica do vestígio, a narrativa do golpe pode existir, mas sua demonstração em juízo se fragiliza de maneira decisiva.

Quanto às plataformas, a pesquisa afastou respostas binárias. A análise mostrou que o grau de intermediação, a arquitetura do serviço e o modo de consumação da fraude influenciam a avaliação de seus deveres jurídicos. Isso exige separar com clareza a responsabilidade do fraudador, que se examina no âmbito penal, das possíveis repercussões civis e regulatórias atribuíveis ao intermediador digital.

Em síntese, um estudo consistente sobre o tema precisa articular quatro eixos: tipificação penal precisa, distinção entre falsa identidade e falsidade ideológica, tratamento técnico da prova digital e delimitação rigorosa dos deveres das plataformas. Quando esses elementos são examinados em conjunto, o debate deixa de ser mera descrição de golpes virtuais e passa a oferecer contribuição efetiva para a compreensão contemporânea do direito penal aplicado aos ecossistemas digitais de compra e venda.

Revista ARACÊ
ISSN: 2358-2472

REFERÊNCIAS

ADVOCACIA-GERAL DA UNIÃO. AGU defende ampliação da responsabilidade de plataformas digitais por conteúdo ilícito de terceiros. Brasília, DF, 28 nov. 2024. Disponível em: https://www.gov.br/agu/pt-br/comunicacao/noticias/agu-defende-ampliacao-da-responsabilidade-de-plataformas-digitais-por-conteudo-ilicito-de-terceiros. Acesso em: 25 mar. 2026.

ARAÚJO, Matheus. Inteligência artificial, blockchain e a cadeia de custódia da prova no processo penal. Revista da Universidade Federal de Minas Gerais, Belo Horizonte, v. 30, 2024. DOI: https://doi.org/10.35699/2965-6931.2023.47605. Disponível em: https://periodicos.ufmg.br/index.php/revistadaufmg/article/view/47605. Acesso em: 28 mar. 2025.

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: 3 mar. 2025.

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/del3689compilado.htm. Acesso em: 4 mar. 2025.

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: 5 mar. 2025.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet. Brasília, DF: Presidência da República, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 6 mar. 2025.

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/l13105.htm. Acesso em: 7 mar. 2025.

BRASIL. Lei nº 13.964, de 24 de dezembro de 2019. Aperfeiçoa a legislação penal e processual penal. Brasília, DF: Presidência da República, 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13964.htm. Acesso em: 19 mar. 2025.

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), e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e dá outras providências. Brasília, DF: Presidência da República, 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2021/Lei/L14155.htm. Acesso em: 2 jun. 2025.

BRASIL. Lei nº 15.229, de 2 de outubro de 2025. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para prever que o estelionato cometido contra pessoa com deficiência procede-se mediante ação penal pública incondicionada. Brasília, DF: Presidência da República, 2025. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2025/Lei/L15229.htm. Acesso em: 7 out. 2025.

Revista ARACÊ
ISSN: 2358-2472

BRITO, Stefhany Sinfrônio. A responsabilização civil dos provedores por anúncios irregulares: uma análise da responsabilidade de redes sociais e marketplaces sob uma perspectiva do Direito do Consumidor. 2023. Trabalho de Conclusão de Curso (Graduação em Direito) – Universidade Federal de Santa Catarina, Florianópolis, 2023. Disponível em: https://repositorio.ufsc.br/handle/123456789/253802. Acesso em: 25 mar. 2025.

CONSELHO NACIONAL DE JUSTIÇA. CNJ debaterá procedimentos para coleta de provas digitais no processo penal. Brasília, DF, 27 maio 2025a. Disponível em: https://www.cnj.jus.br/cnj-debatera-procedimentos-para-coleta-de-provas-digitais-no-processo-penal/. Acesso em: 29 maio 2025.

CONSELHO NACIONAL DE JUSTIÇA. Seminário sobre provas digitais. Brasília, DF, 28 maio 2025b. Disponível em: https://www.cnj.jus.br/agendas/seminario-sobre-provas-digitais/. Acesso em: 30 maio 2025.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. 19º Anuário Brasileiro de Segurança Pública 2025. São Paulo: FBSP, 2025. Disponível em: https://forumseguranca.org.br/anuario-brasileiro-seguranca-publica/. Acesso em: 29 jul. 2025.

SAAD, Marta; ROSSI, Helena Costa; PARTATA, Pedro Henrique. A obtenção das provas digitais no processo penal demanda uma disciplina jurídica própria? Uma análise do conceito, das características e das peculiaridades das provas digitais. Revista Brasileira de Direito Processual Penal, Porto Alegre, v. 10, n. 3, 2024. DOI: https://doi.org/10.22197/rbdpp.v10i3.1071. Disponível em: https://revista.ibraspp.com.br/RBDPP/article/view/1071. Acesso em: 31 mar. 2025.

SENADO FEDERAL. Projeto de Lei nº 4.103, de 2024. Altera a Lei nº 12.965, de 23 de abril de 2014, para dispor sobre aplicações de publicação de anúncios e de intermediação de operações de compra e venda entre usuários pela internet. Brasília, DF, 2024. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/165939. Acesso em: 28 abr. 2025.

SERASA EXPERIAN. O mapa da fraude no Brasil: mapa de fraude novembro 2021. São Paulo, nov. 2021. Disponível em: https://www.serasa.com.br/premium/blog/mapa-da-fraude/. Acesso em: 17 mar. 2025.

SERASA EXPERIAN. Tentativas de fraude contra idosos aumentam em quase 12% em 2024, revela Serasa Experian. São Paulo, 19 mar. 2025e. Disponível em: https://www.serasaexperian.com.br/sala-de-imprensa/prevencao-a-fraude/tentativas-de-fraude-contra-idosos-aumentam-em-quase-12-em-2024-revela-serasa-experian/. Acesso em: 20 mar. 2025.

SERASA EXPERIAN. Brasil registra mais de 1 milhão de tentativas de fraude pelo segundo mês consecutivo em 2025, revela Serasa Experian. São Paulo, 16 maio 2025c. Disponível em: https://www.serasaexperian.com.br/sala-de-imprensa/indicadores/brasil-registra-mais-de-1-milhao-de-tentativas-de-fraude-pelo-segundo-mes-consecutivo-em-2025-revela-serasa-experian/. Acesso em: 20 maio 2025.

SERASA EXPERIAN. Tentativas de fraude crescem 22,9% no 1º trimestre de 2025 em comparação ao mesmo período de 2024, revela Serasa Experian. São Paulo, 23 jun. 2025a. Disponível em: https://www.serasaexperian.com.br/sala-de-imprensa/prevencao-a-fraude/tentativas-de-fraude-

Revista ARACÊ
ISSN: 2358-2472

crescem-229-no-1-trimestre-de-2025-em-comparacao-ao-mesmo-periodo-de-2024-revela-serasa-experian/. Acesso em: 24 jun. 2025.

SERASA EXPERIAN. Tentativas de golpe envolvendo biometria e documento falso aumentam quase 30% em um ano, segundo Serasa Experian; veja como se proteger. São Paulo, 25 ago. 2025d. Disponível em: https://www.serasaexperian.com.br/sala-de-imprensa/prevencao-a-fraude/tentativas-de-golpe-envolvendo-biometria-e-documento-falso-aumentam-quase-30-em-um-ano-segundo-serasa-experian-veja-como-se-proteger/. Acesso em: 26 ago. 2025.

SERASA EXPERIAN. Recorde: quase 7 milhões de tentativas de fraude foram registradas no 1º semestre de 2025; setor bancário é principal alvo. São Paulo, 30 set. 2025b. Disponível em: https://www.serasaexperian.com.br/sala-de-imprensa/indicadores/recorde-quase-7-milhoes-de-tentativas-de-fraude-foram-registradas-no-1-semestre-de-2025-setor-bancario-e-principal-alvo/. Acesso em: 2 out. 2025.

SERASA EXPERIAN. Tipos de biometria: qual deles é o mais seguro do mercado? São Paulo, 22 jan. 2026. Disponível em: https://www.serasaexperian.com.br/conteudos/tipos-de-biometria-qual-deles-e-o-mais-seguro-do-mercado/. Acesso em: 4 abr. 2026.

SUPERIOR TRIBUNAL DE JUSTIÇA. Súmula 17. Quando o falso se exaure no estelionato, sem mais potencialidade lesiva, é por este absorvido. Brasília, DF, 28 nov. 1990. Disponível em: https://www.stj.jus.br/docs_internet/VerbetesSTJ_asc.pdf. Acesso em: 10 mar. 2025.

SUPERIOR TRIBUNAL DE JUSTIÇA. Site de comércio eletrônico não é responsável por fraude praticada fora da plataforma. Brasília, DF, 8 abr. 2021a. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/08042021-Site-de-comercio-eletronico-nao-e-responsavel-por-fraude-praticada-fora-da-plataforma.aspx. Acesso em: 15 abr. 2025.

SUPERIOR TRIBUNAL DE JUSTIÇA. Lei 14.155/2021 só alterou competência para julgamento de estelionato em casos específicos. Brasília, DF, 30 maio 2022. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/30052022-Lei-14-5552021-so-alterou-competencia-para-julgamento-de-estelionato-em-casos-especificos.aspx. Acesso em: 23 out. 2025.

SUPERIOR TRIBUNAL DE JUSTIÇA. Quinta Turma não aceita como provas prints de celular extraídos sem metodologia adequada. Brasília, DF, 2 maio 2024a. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2024/02052024-Quinta-Turma-nao-aceita-como-provas-prints-de-celular-extraidos-sem-metodologia-adequada.aspx. Acesso em: 9 maio 2025.

SUPERIOR TRIBUNAL DE JUSTIÇA. Crime de falsa identidade não exige obtenção de vantagem e se consuma no ato de fornecer dado incorreto. Brasília, DF, 17 jun. 2025a. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2025/17062025-Crime-de-falsa-identidade-nao-exige-obtencao-de-vantagem-e-se-consuma-no-ato-de-fornecer-dado-incorreto.aspx. Acesso em: 18 jun. 2025.

SUPREMO TRIBUNAL FEDERAL. STF define parâmetros para responsabilização de plataformas por conteúdos de terceiros. Brasília, DF, 26 jun. 2025. Disponível em:

Revista ARACÊ
ISSN: 2358-2472

https://noticias.stf.jus.br/postsnoticias/stf-define-parametros-para-responsabilizacao-de-plataformas-por-conteudos-de-terceiros/. Acesso em: 27 jun. 2025.

VAZ, Denise Provasi. Provas digitais no processo penal: formulação do conceito, definição das características e sistematização do procedimento probatório. 2012. Tese (Doutorado em Direito Processual) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2012. Disponível em: https://teses.usp.br/teses/disponiveis/2/2137/tde-28052013-153123/pt-br.php. Acesso em: 2 abr. 2025.