BOCA
BOLETIM DE CONJUNTURA

RESPONSABILIDADE CIVIL NA ERA DIGITAL: FRAUDES ELETRÔNICAS, DANO MORAL E DECISÕES ALGORÍTMICAS

CIVIL LIABILITY IN THE DIGITAL AGE: ELECTRONIC FRAUD, MORAL DAMAGES, AND ALGORITHMIC DECISIONS

RESPONSABILIDAD CIVIL EN LA ERA DIGITAL: FRAUDE ELECTRÓNICO, DAÑOS MORALES Y DECISIONES ALGORÍTMICAS

10.56238/bocav25n79-030

Vinicius Martins Ferreira
Pós-graduado
Orientador
E-mail: correspondentems2021@gmail.com

Telma Salgueiro Braga de Lima
Graduando em Direito
Instituição: Unigran Capital
E-mail: telmasalgueiro@gmail.com

Barbara Sabrine Lima Moura
Graduando em Direito
Instituição: Unigran Capital
E-mail: barbarasabrine@gmail.com

Carlos Rodrigues Sandim
Graduando em Direito
Instituição: Unigran Capital
E-mail: carlosrodriguessandim@gmail.com

Aline de Almeida Bugenski
Graduando em Direito
Instituição: Unigran Capital
E-mail: alinebugenski@gmail.com

Dulce Ferreira de Oliveira
Graduando em Direito
Instituição: Unigran Capital
E-mail: dulceferreiradeoliveira@gmail.com

Pedro Henrique Maciel Ribeiro
Graduando em Direito
Instituição: Unigran Capital
E-mail: pedromacielribeiro@gmail.com

RESUMO

O presente estudo teve como objetivo geral analisar a responsabilidade civil na era digital, considerando três frentes centrais: as fraudes eletrônicas nas relações de consumo, o dano moral produzido em ambientes virtuais e os prejuízos decorrentes de decisões algorítmicas. Como objetivos específicos, buscou-se examinar a evolução da responsabilidade civil da culpa à teoria do risco, compreender o papel do dever de segurança nas transações digitais, identificar critérios para diferenciar crítica legítima e ilícito civil indenizável nas redes sociais e avaliar os desafios da causalidade diante da opacidade dos sistemas automatizados. A pesquisa foi desenvolvida por meio de revisão bibliográfica, com abordagem qualitativa, a partir de doutrina civilista, legislação brasileira, precedentes consolidados e discussões regulatórias contemporâneas. O estudo evidenciou que os pressupostos clássicos da responsabilidade civil permanecem relevantes, mas precisam ser reinterpretados diante da multiplicidade de agentes, da assimetria informacional, da viralização de conteúdos, da automação decisória e da dificuldade probatória própria do ambiente digital. Constatou-se que a responsabilidade objetiva, fundada no risco da atividade e no dever de segurança, tende a assumir centralidade em fraudes bancárias, comércio eletrônico e serviços intermediados por plataformas. Também se verificou que o dano moral digital não se limita ao conteúdo ofensivo originário, pois sua intensidade decorre da difusão, persistência, replicação e exposição pública continuada. Quanto às decisões algorítmicas, observou-se que a opacidade técnica e a autonomia relativa dos sistemas exigem parâmetros como transparência, explicabilidade, auditoria, rastreabilidade e supervisão humana. Conclui-se que a tutela civil na era digital deve combinar reparação, prevenção, governança tecnológica e proteção efetiva dos direitos fundamentais.

Palavras-chave: Responsabilidade Civil. Fraudes Digitais. Dano Moral. Inteligência Artificial. Direitos da Personalidade.

ABSTRACT

This study aimed to analyze civil liability in the digital age, considering three central dimensions: electronic fraud in consumer relations, moral damages produced in virtual environments, and harm resulting from algorithmic decisions. Specifically, it sought to examine the evolution of civil liability from fault to risk theory, understand the role of the duty of security in digital transactions, identify criteria to distinguish legitimate criticism from compensable civil wrongs on social networks, and evaluate causation challenges arising from the opacity of automated systems. The research was developed through a bibliographic review, using a qualitative approach based on civil law doctrine, Brazilian legislation, consolidated precedents, and contemporary regulatory debates. The study showed that traditional elements of civil liability remain relevant but must be reinterpreted in light of multiple actors, informational asymmetry, content virality, automated decision-making, and evidentiary difficulties in digital environments. It found that strict liability, based on business risk and the duty of security, tends to play a central role in banking fraud, e-commerce, and platform-mediated services. It also observed that digital moral damage is not limited to the original offensive content, since its intensity depends on dissemination, persistence, replication, and continued public exposure. Regarding algorithmic decisions, technical opacity and the relative autonomy of systems require standards such as transparency, explainability, auditing, traceability, and human oversight. It concludes that civil protection in the digital age must combine compensation, prevention, technological governance, and effective protection of fundamental rights.

Keywords: Civil Liability. Digital Fraud. Moral Damages. Artificial Intelligence. Personality Rights.

RESUMEN

Este estudio tuvo como objetivo analizar la responsabilidad civil en la era digital, considerando tres áreas centrales: el fraude electrónico en las relaciones con los consumidores, los daños morales producidos en entornos virtuales y las pérdidas derivadas de decisiones algorítmicas. Específicamente, buscó examinar la evolución de la responsabilidad civil desde la teoría de la culpa a la teoría del riesgo, comprender el rol del deber de seguridad en las transacciones digitales, identificar criterios para diferenciar la crítica legítima de los daños civiles indemnizables en las redes sociales y evaluar los desafíos de la causalidad ante la opacidad de los sistemas automatizados. La investigación se desarrolló a través de una revisión bibliográfica, con un enfoque cualitativo, basada en la doctrina del derecho civil, la legislación brasileña, precedentes consolidados y debates regulatorios contemporáneos. El estudio demostró que los supuestos clásicos de la responsabilidad civil siguen siendo relevantes, pero necesitan ser reinterpretados a la luz de la multiplicidad de agentes, la asimetría de la información, el contenido viral, la automatización de la toma de decisiones y las dificultades probatorias inherentes al entorno digital. Se encontró que la responsabilidad objetiva, basada en el riesgo de la actividad y el deber de seguridad, tiende a adquirir centralidad en el fraude bancario, el comercio electrónico y los servicios mediados por plataformas. También se constató que el daño moral digital no se limita al contenido ofensivo original, ya que su intensidad proviene de la difusión, la persistencia, la replicación y la continua exposición pública. En cuanto a las decisiones algorítmicas, se observó que la opacidad técnica y la relativa autonomía de los sistemas requieren parámetros como la transparencia, la explicabilidad, la auditabilidad, la trazabilidad y la supervisión humana. Se concluye que la protección civil en la era digital debe combinar la reparación, la prevención, la gobernanza tecnológica y la protección efectiva de los derechos fundamentales.

Palabras clave: Responsabilidad Civil. Fraude Digital. Daño Moral. Inteligencia Artificial. Derechos de la Personalidad.

1 INTRODUÇÃO

A consolidação das tecnologias digitais transformou a forma como pessoas contratam, consomem, se expressam, trabalham e exercem seus direitos. O comércio eletrônico, os meios de pagamento instantâneos, as redes sociais, os marketplaces, os aplicativos de transporte, os sistemas de recomendação e as ferramentas de inteligência artificial passaram a integrar o cotidiano de forma estrutural. Como consequência, a responsabilidade civil deixou de lidar apenas com danos decorrentes de condutas individualizadas e passou a enfrentar danos produzidos por cadeias tecnológicas complexas, marcadas por múltiplos agentes, fluxos informacionais e riscos distribuídos (Gagliano; Pamplona Filho, 2026).

O ambiente digital amplia oportunidades econômicas e comunicacionais, mas também intensifica vulnerabilidades. O consumidor que realiza uma compra online, utiliza Pix, acessa uma plataforma ou confia em anúncio veiculado por influenciador não domina a estrutura técnica por trás da operação. A assimetria informacional torna-se ainda mais acentuada quando a relação envolve algoritmos, autenticação multifator, análise automatizada de risco, sistemas antifraude, gateways de pagamento e políticas internas de plataformas (Miragem, 2024).

No campo das fraudes digitais, a responsabilidade civil enfrenta o desafio de definir quem deve suportar o prejuízo quando há golpe de engenharia social, boleto adulterado, invasão de conta, compra não entregue, abertura fraudulenta de conta bancária ou transação atípica não bloqueada. A resposta tradicional baseada na culpa individual mostra-se insuficiente quando a fraude decorre de falhas sistêmicas de segurança, de omissões de monitoramento ou da exploração de vulnerabilidades previsíveis do próprio serviço (Cavalieri Filho, 2023).

No campo do dano moral digital, o problema assume outra feição. A ofensa à honra, à imagem, à privacidade ou à intimidade deixa de ser um episódio isolado e passa a circular em redes de replicação, comentários, compartilhamentos, prints, repostagens e mecanismos de recomendação. A lesão não se esgota no ato inicial, pois pode permanecer disponível, ser reativada por buscas, alcançar públicos indeterminados e produzir estigmatização prolongada (Schreiber, 2021).

A cultura do cancelamento, os ataques coordenados e a exposição massiva evidenciam que a liberdade de expressão deve ser compatibilizada com os direitos da personalidade. A crítica pública, ainda que dura, integra o debate democrático; contudo, a manifestação deixa de ser legítima quando assume caráter abusivo, persecutório, discriminatório, desproporcional ou voltado à destruição reputacional do indivíduo. A responsabilidade civil, nesse contexto, deve distinguir crítica, opinião e denúncia de linchamento digital indenizável (Tartuce, 2025).

A terceira frente de análise diz respeito às decisões algorítmicas. Sistemas de inteligência artificial já auxiliam na concessão de crédito, no ranqueamento de conteúdos, na seleção de candidatos, no bloqueio de contas, na detecção de fraudes, na análise de documentos e até na organização de dados

jurídicos. Quando tais sistemas produzem danos, a imputação de responsabilidade se torna mais difícil, pois o resultado pode decorrer de bases de dados, escolhas de desenvolvimento, modelos estatísticos, critérios de treinamento e decisões automatizadas opacas (Calo, 2017).

A opacidade algorítmica desloca o problema da responsabilidade civil para uma dimensão probatória e regulatória. Se o sujeito lesado não consegue compreender por que foi bloqueado, excluído, negativado, classificado como fraudador ou prejudicado por decisão automatizada, torna-se difícil reconstruir a causalidade e demonstrar a falha. Por isso, transparência, explicabilidade, rastreabilidade, auditoria e supervisão humana passam a funcionar como condições jurídicas para a efetividade da reparação (Floridi, 2021).

Diante desse cenário, o presente estudo parte do seguinte problema de pesquisa: de que forma a responsabilidade civil brasileira deve ser reinterpretada para tutelar fraudes digitais, dano moral nas redes e decisões algorítmicas sem comprometer a inovação tecnológica e a liberdade de expressão?

O objetivo geral consiste em analisar a responsabilidade civil na era digital a partir de três eixos: fraudes eletrônicas nas relações de consumo, dano moral em ambientes virtuais e decisões algorítmicas. Como objetivos específicos, busca-se examinar a evolução da culpa para o risco, identificar deveres de segurança das plataformas e instituições financeiras, propor critérios para aferição do dano moral digital e analisar os desafios de causalidade em sistemas automatizados.

A pesquisa justifica-se pela crescente judicialização de conflitos digitais e pela necessidade de parâmetros mais seguros para orientar consumidores, fornecedores, plataformas, instituições financeiras, usuários de redes sociais e operadores do Direito. A ausência de critérios claros favorece decisões contraditórias, insegurança jurídica e transferência indevida de riscos tecnológicos às vítimas (Marques, 2023).

Quanto à metodologia, o estudo adota abordagem qualitativa, de natureza exploratória e descritiva, desenvolvida por meio de revisão bibliográfica e análise normativa. Utilizam-se doutrinas de responsabilidade civil, direito do consumidor, direitos da personalidade, proteção de dados e regulação digital, bem como legislação brasileira pertinente, especialmente o Código Civil, o Código de Defesa do Consumidor, o Marco Civil da Internet e a Lei Geral de Proteção de Dados.

2 A RESPONSABILIDADE CIVIL NA SOCIEDADE DIGITAL

2.1 DA CULPA AO RISCO NAS RELAÇÕES TECNOLÓGICAS

A responsabilidade civil brasileira tem como ponto de partida a ideia de reparação do dano injusto. No modelo clássico, a obrigação de indenizar vinculava-se à comprovação de conduta culposa, dano e nexo causal, em consonância com os arts. 186 e 927 do Código Civil. Essa estrutura continua relevante, mas não é suficiente para todas as hipóteses contemporâneas, especialmente quando a vítima

não possui acesso às informações necessárias para demonstrar a culpa do agente econômico ou tecnológico (Diniz, 2019).

A evolução da responsabilidade civil revela progressivo deslocamento da culpa para o risco. O parágrafo único do art. 927 do Código Civil admite responsabilidade independentemente de culpa quando a atividade normalmente desenvolvida implicar risco para direitos de terceiros. Essa abertura normativa permite adaptar o instituto a atividades digitais que, embora socialmente úteis, criam riscos massificados de fraude, vazamento, exposição e erro automatizado (Gonçalves, 2019).

No ambiente de consumo, essa evolução é ainda mais expressiva. O art. 14 do Código de Defesa do Consumidor estabelece responsabilidade objetiva do fornecedor pelos danos decorrentes de defeitos na prestação de serviço, inclusive por informações insuficientes ou inadequadas. Tal regra ganha importância no comércio eletrônico, pois o consumidor depende da infraestrutura técnica do fornecedor para contratar, pagar, receber e reclamar (Miragem, 2024).

A teoria do risco do empreendimento assume papel central quando a atividade econômica se beneficia da digitalização. Bancos, marketplaces, plataformas de anúncios, gateways de pagamento, empresas antifraude e operadores logísticos lucram com a eficiência, escala e automação do mercado digital. Por isso, devem internalizar os riscos ordinários da atividade, em vez de transferi-los automaticamente ao consumidor vulnerável (Cavalieri Filho, 2023).

A culpa não desaparece, mas deixa de ocupar posição exclusiva. Em fraudes digitais, a análise da culpa individual do consumidor deve ser feita com cautela, pois golpes sofisticados exploram engenharia social, interfaces enganosas, semelhança visual com canais oficiais e confiança legítima em sistemas digitais. A responsabilização não pode ignorar a vulnerabilidade técnica e informacional do usuário comum (Marques, 2023).

A passagem do modelo subjetivo para regimes objetivos também se explica pela função preventiva da responsabilidade civil. Reparar o dano é importante, mas prevenir sua ocorrência é ainda mais relevante quando se trata de danos digitais, que podem atingir milhares de pessoas em segundos e produzir efeitos econômicos e reputacionais de difícil reversão (Tartuce, 2025).

A responsabilidade civil contemporânea, portanto, deve ser compreendida como instrumento de distribuição de riscos sociais. Quem estrutura, controla e explora economicamente ambiente digital deve demonstrar que adotou padrões adequados de segurança, informação, prevenção e resposta. Essa compreensão aproxima o instituto da lógica constitucional de proteção da dignidade humana e da confiança nas relações privadas (Schreiber, 2021).

2.2 A CENTRALIDADE DO DEVER DE SEGURANÇA

O dever de segurança tornou-se elemento nuclear da responsabilidade civil digital. Em relações presenciais, o consumidor pode examinar parte do produto, conferir documentos ou interagir

diretamente com o fornecedor. No ambiente digital, sua confiança é depositada na interface, na autenticação, na reputação da plataforma, no sistema de pagamento e nas promessas de segurança divulgadas pelo fornecedor (Miragem, 2024).

A segurança digital não se limita à proteção técnica contra invasões. Ela compreende deveres de informação clara, arquitetura de prevenção, detecção de operações atípicas, controle de identidade, monitoramento antifraude, canais efetivos de atendimento, resposta rápida a incidentes e redução de danos. A omissão em qualquer dessas etapas pode configurar defeito do serviço (Doneda; Mendes, 2024).

A Lei Geral de Proteção de Dados reforça essa compreensão ao exigir medidas técnicas e administrativas aptas a proteger dados pessoais contra acessos não autorizados e situações acidentais ou ilícitas. Ainda que a LGPD tenha objeto próprio, sua lógica preventiva dialoga com a responsabilidade civil, pois a falha de segurança informacional pode ser causa direta de fraudes, golpes, exposição indevida e danos morais (Bioni, 2018).

O Marco Civil da Internet também contribui para esse cenário ao estabelecer princípios, garantias e deveres para o uso da internet no Brasil. Embora o regime de responsabilidade de provedores por conteúdo de terceiros tenha regra própria, a lei reforça valores como privacidade, proteção de dados, preservação da estabilidade da rede e responsabilidade dos agentes conforme suas atividades (Leonardi, 2019).

O dever de segurança possui dimensão objetiva porque não depende apenas da intenção do fornecedor. Uma plataforma pode não desejar a fraude, mas responde quando sua estrutura facilita a prática ilícita, deixa de impedir operação claramente atípica ou não oferece mecanismos mínimos de controle. A boa-fé subjetiva do fornecedor não elimina o defeito do serviço quando o risco era inerente à atividade (Cavalieri Filho, 2023).

A segurança por design deve ser compreendida como parâmetro de diligência qualificada. Empresas que atuam digitalmente precisam construir seus serviços considerando o risco de fraude desde a concepção, e não apenas reagir após a lesão. Essa lógica exige avaliação de risco, testes de vulnerabilidade, monitoramento contínuo e mecanismos de mitigação de danos (Doneda; Mendes, 2024).

A responsabilidade civil, nessa perspectiva, opera como incentivo institucional. Ao imputar o custo dos danos aos agentes que melhor podem preveni-los, o Direito estimula investimentos em segurança, reduz externalidades negativas e protege a confiança social no ambiente digital (Miragem, 2024).

2.3 A MULTIPLICIDADE DE AGENTES E O PROBLEMA DA CADEIA DIGITAL

A cadeia digital raramente envolve apenas consumidor e fornecedor direto. Em uma compra online, podem atuar marketplace, vendedor, banco emissor, instituição recebedora, gateway de pagamento, empresa antifraude, operador logístico, plataforma de anúncios, influenciador digital e provedor de aplicação. Essa multiplicidade dificulta a identificação do responsável, mas não pode servir como obstáculo à reparação da vítima (Marques, 2023).

O Código de Defesa do Consumidor adota lógica de solidariedade entre integrantes da cadeia de fornecimento. Essa orientação é especialmente adequada ao ambiente digital, no qual o consumidor não consegue distinguir com precisão a função técnica de cada agente. A confiança é projetada sobre o ecossistema inteiro, e não apenas sobre a empresa que aparece formalmente no contrato (Miragem, 2024).

As plataformas digitais frequentemente se apresentam como intermediárias neutras, mas sua atuação pode ser mais intensa. Quando organizam a oferta, controlam reputação, processam pagamento, retêm valores, disponibilizam logística, ranqueiam produtos e capturam comissão, deixam de ser meros espaços passivos e passam a integrar a cadeia de consumo de forma relevante (Marques, 2023).

O mesmo raciocínio se aplica aos gateways e empresas antifraude. Esses agentes não apenas viabilizam tecnicamente pagamentos; eles oferecem confiança, validação e proteção contra riscos. Se sua atividade promete segurança e reduz fricções na transação, também deve responder quando falhas sistêmicas contribuem para o dano (Miragem, 2024).

As instituições financeiras ocupam posição ainda mais sensível. A Súmula 479 do Superior Tribunal de Justiça consolidou que elas respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias. A digitalização dos pagamentos não reduz essa responsabilidade, mas amplia o dever de monitorar operações atípicas (Schreiber, 2025).

A fragmentação técnica da cadeia não pode gerar fragmentação da tutela. A vítima não deve suportar o ônus de descobrir internamente qual sistema falhou, qual algoritmo aprovou a transação, qual banco recebeu o valor ou qual fornecedor deixou de verificar a identidade do fraudador. A solidariedade permite posterior direito de regresso entre os responsáveis, preservando a efetividade da reparação (Cavalieri Filho, 2023).

Por isso, a responsabilidade civil digital deve ser funcional: deve buscar quem criou, controlou, explorou ou melhor poderia prevenir o risco. Essa diretriz evita que a complexidade tecnológica se transforme em escudo de irresponsabilidade (Tartuce, 2025).

3 FRAUDES DIGITAIS NAS RELAÇÕES DE CONSUMO

3.1 BANCOS, PIX E FORTUITO INTERNO

As fraudes bancárias digitais representam um dos principais campos de aplicação da responsabilidade objetiva na sociedade contemporânea. Transferências por Pix, boletos fraudulentos, abertura indevida de contas, invasão de aplicativos, golpes por telefone e engenharia social tornaram-se recorrentes. Embora terceiros pratiquem o ato ilícito imediato, o risco integra a atividade bancária digital quando há falha de segurança, monitoramento ou resposta (Schreiber, 2025).

A prestação de serviços financeiros exige padrões elevados de segurança. Bancos operam com dados sensíveis, movimentam patrimônio de terceiros e possuem tecnologia capaz de identificar padrões incomuns. Por isso, transações incompatíveis com o perfil do consumidor, realizadas em curto intervalo, para contas recém-criadas ou em valores atípicos devem acionar mecanismos de alerta, confirmação ou bloqueio (Doneda; Mendes, 2024).

A senha ou autenticação não encerra a análise de responsabilidade. Em golpes sofisticados, o consumidor pode ser induzido a confirmar operação sem compreender a fraude. A utilização de credenciais pessoais é elemento relevante, mas não afasta automaticamente o defeito do serviço quando o banco deixou de detectar operação anômala ou não disponibilizou canal eficiente de contenção (Cavalieri Filho, 2023).

O fortuito interno corresponde justamente ao risco previsível da atividade. Fraudes praticadas por terceiros no ambiente bancário não são eventos completamente estranhos ao serviço, pois bancos estruturam sua atividade em ambiente sujeito a ataques, falsificações, engenharia social e tentativa de invasão. Por isso, devem investir continuamente em mecanismos preventivos (Miragem, 2024).

A exclusão de responsabilidade somente se justifica quando houver prova robusta de culpa exclusiva da vítima ou fortuito externo. Essa prova deve demonstrar que o dano decorreu de comportamento completamente alheio ao serviço, sem qualquer contribuição de falha sistêmica. A interpretação restritiva da excludente preserva o equilíbrio da relação de consumo e impede transferência indevida do risco ao usuário (Marques, 2023).

A responsabilidade bancária digital também possui dimensão pedagógica. A indenização não deve apenas recompor o patrimônio do consumidor, mas estimular a instituição a aprimorar autenticação, monitoramento, educação digital, bloqueios preventivos e protocolos de devolução de valores. A confiança no sistema financeiro depende de resposta eficiente às fraudes (Schreiber, 2025).

3.2 MARKETPLACES, OFERTAS E INTERMEDIAÇÃO ATIVA

Os marketplaces alteraram profundamente o comércio eletrônico. Ao reunir vendedores, consumidores, meios de pagamento, reputação, avaliações, garantias, anúncios e logística, essas plataformas criam ambiente de confiança que induz o consumidor a contratar. A questão jurídica

central é saber quando a plataforma responde por fraudes, inadimplementos ou falhas de terceiros vendedores (Marques, 2023).

A plataforma que apenas hospeda anúncio, sem intervir na transação, pode ter responsabilidade mais limitada. Contudo, quando participa ativamente da operação, recebe comissão, gerencia pagamento, controla reputação, oferece garantia, organiza entrega ou promove o vendedor, sua posição deixa de ser neutra. Nesses casos, integra a cadeia de fornecimento e responde solidariamente por defeitos do serviço (Miragem, 2024).

A vinculação da oferta assume papel importante nesse contexto. O art. 30 do Código de Defesa do Consumidor estabelece que informação ou publicidade suficientemente precisa obriga o fornecedor. Em ambiente digital, descrições de produto, prazos de entrega, selos de segurança, avaliações, garantias e políticas de reembolso formam a expectativa legítima do consumidor (Marques, 2023).

A publicidade enganosa ou omissa em plataforma digital pode produzir dano de grande escala. A interface pode destacar preço, urgência, desconto ou confiabilidade sem revelar riscos, limitações, vendedor duvidoso ou condições relevantes. A omissão de informação essencial viola o dever de transparência e pode caracterizar defeito do serviço (Tartuce, 2025).

No caso de não entrega de produto, produto falso, golpe de vendedor cadastrado ou desvio de pagamento, deve-se analisar se a plataforma criou aparência de segurança e se lucrou com a intermediação. Quanto maior o controle sobre a operação, maior tende a ser a responsabilidade. A posição econômica da plataforma justifica deveres proporcionais de verificação e resposta (Miragem, 2024).

A responsabilidade dos marketplaces deve equilibrar proteção do consumidor e viabilidade econômica. Não se trata de atribuir responsabilidade ilimitada por qualquer fraude externa, mas de reconhecer que plataformas ativas não podem se beneficiar da confiança que constroem e, ao mesmo tempo, negar responsabilidade quando essa confiança é frustrada por falha do ecossistema (Marques, 2023).

3.3 GATEWAYS, ANTIFRAUDE E LOGÍSTICA

Os gateways de pagamento e empresas antifraude ocupam posição técnica, mas juridicamente relevante. São eles que processam pagamentos, validam transações, analisam risco, aprovam compras e bloqueiam operações suspeitas. Quando esses serviços falham, o dano pode atingir consumidor, lojista ou ambos, exigindo análise da função concreta desempenhada na cadeia digital (Miragem, 2024).

A promessa de antifraude não pode ser meramente publicitária. Se determinada empresa oferece solução de análise de risco, espera-se que adote critérios minimamente eficazes para identificar

padrões incompatíveis, cartões suspeitos, divergência de dados, múltiplas tentativas e comportamento atípico. A falha grosseira na detecção pode configurar defeito do serviço (Cavalieri Filho, 2023).

Contratos que transferem integralmente ao lojista ou consumidor o risco de chargeback, fraude ou contestação devem ser examinados à luz da boa-fé objetiva e do equilíbrio contratual. O fornecedor técnico que controla ferramentas de prevenção não pode deslocar todo o prejuízo a quem não possui acesso aos parâmetros internos do sistema (Tartuce, 2025).

As empresas de logística também integram a confiança do comércio eletrônico. A entrega é etapa essencial do contrato, e o consumidor não separa a compra da entrega. Extravio, entrega a terceiro não autorizado, violação de embalagem ou ausência de rastreamento adequado podem caracterizar falha do serviço, especialmente quando a logística é oferecida como parte da operação integrada (Marques, 2023).

O transporte de mercadorias em ambiente de consumo digital não é atividade acessória irrelevante. O consumidor paga pelo resultado final: receber o produto adquirido. Por isso, varejista, marketplace e transportadora podem responder solidariamente quando a cadeia de entrega falha e impede a fruição do bem (Miragem, 2024).

A análise jurídica deve evitar que cada integrante da cadeia atribua a culpa ao outro. A solidariedade protege a vítima e permite que os responsáveis discutam internamente o grau de participação. Essa solução é coerente com a teoria do risco e com a finalidade protetiva do Direito do Consumidor (Cavalieri Filho, 2023).

3.4 INFLUENCIADORES DIGITAIS E PUBLICIDADE DE CONFIANÇA

Influenciadores digitais exercem papel relevante na formação da vontade do consumidor. Diferentemente da publicidade tradicional, sua mensagem é percebida como recomendação pessoal, experiência autêntica ou conselho de alguém próximo. Essa aparência de espontaneidade aumenta o poder persuasivo e, por consequência, o dever de transparência (Marques, 2023).

Quando o influenciador divulga produto ou serviço mediante remuneração, permuta ou vantagem econômica, sua atuação deve ser identificada de forma clara. A omissão sobre o caráter publicitário viola o dever de informação e pode induzir o consumidor a acreditar que está diante de opinião independente. Em ambiente digital, a confiança pessoal é parte do mecanismo de venda (Miragem, 2024).

A responsabilidade do influenciador deve ser analisada conforme o grau de participação. Quem apenas reproduz anúncio genérico pode ter responsabilidade distinta daquele que afirma ter testado produto, promete resultado, minimiza risco ou recomenda investimento financeiro. Quanto maior o endosso pessoal, maior o dever de diligência informativa (Tartuce, 2025).

Publicidade de produtos financeiros, cursos, apostas, suplementos, procedimentos estéticos e investimentos exige cuidado especial. Nesses setores, o risco de dano patrimonial e moral é elevado, e o público pode ser vulnerável. A popularidade do influenciador não pode funcionar como escudo para divulgação negligente ou enganosa (Marques, 2023).

A responsabilização de influenciadores não representa censura à liberdade de expressão. Trata-se de aplicar às práticas comerciais digitais os mesmos valores de transparência, boa-fé e proteção da confiança que regem a publicidade em geral. A liberdade de recomendar não elimina o dever de informar corretamente quando há relação econômica envolvida (Miragem, 2024).

4 DANO MORAL DIGITAL E DIREITOS DA PERSONALIDADE

4.1 HONRA, IMAGEM E PRIVACIDADE EM AMBIENTE DE REDE

Os direitos da personalidade protegem dimensões essenciais da pessoa, como honra, imagem, nome, privacidade, intimidade e identidade. No ambiente digital, esses direitos sofrem novas formas de ameaça, pois a circulação de informações é rápida, massiva, replicável e persistente. O dano moral digital deve ser compreendido a partir dessa dinâmica própria (Schreiber, 2021).

A ofensa publicada na internet pode atingir públicos indeterminados, ultrapassar fronteiras territoriais e permanecer acessível por tempo prolongado. Ainda que o conteúdo original seja removido, cópias, prints, republicações e indexações podem manter a lesão viva. Essa persistência diferencia o dano digital de muitas ofensas presenciais ou restritas a círculos limitados (Tartuce, 2025).

A honra objetiva é afetada quando a reputação social da pessoa é diminuída perante terceiros. A honra subjetiva, por sua vez, relaciona-se ao sentimento íntimo de dignidade. Nas redes sociais, ambas podem ser atingidas de forma simultânea, especialmente quando há imputações falsas, insultos, exposição vexatória ou divulgação de informações íntimas (Gagliano; Pamplona Filho, 2026).

A privacidade também assume contornos específicos. Dados pessoais, fotos, conversas, localização, hábitos de consumo, histórico profissional e preferências podem ser expostos sem autorização. A LGPD reforça a compreensão de que dados pessoais integram esfera de proteção da pessoa natural, e sua utilização indevida pode gerar dano patrimonial ou moral (Bioni, 2018).

O dano moral digital não deve ser presumido em qualquer dissabor online. A banalização da indenização enfraquece a responsabilidade civil. Contudo, também não se pode exigir prova impossível de sofrimento íntimo em casos de exposição pública grave, vazamento de dados sensíveis, discurso discriminatório ou ataque coordenado à reputação (Schreiber, 2021).

O intérprete deve avaliar contexto, conteúdo, alcance, intenção, repercussão e persistência. A análise isolada da frase ofensiva pode ser insuficiente, porque o dano digital decorre muitas vezes do ambiente de circulação, da audiência alcançada e do modo como terceiros aderem à exposição (Tartuce, 2025).

4.2 CRÍTICA LEGÍTIMA, LIBERDADE DE EXPRESSÃO E ILÍCITO CIVIL

A liberdade de expressão é direito fundamental indispensável ao debate público, ao controle social e à democracia. Críticas a agentes públicos, empresas, profissionais e influenciadores podem ser contundentes, irônicas ou severas sem necessariamente configurar ilícito civil. O Direito não deve transformar qualquer desconforto reputacional em indenização (Vieira, 2019).

A crítica legítima, porém, possui limites. Ela deve manter conexão com fatos, opiniões ou temas de interesse público, sem descambar para ofensas pessoais gratuitas, acusações falsas, discurso de ódio, perseguição coordenada ou exposição de informações íntimas irrelevantes. O abuso do direito de expressão pode gerar responsabilidade civil (Schreiber, 2021).

A distinção entre crítica e ilícito exige critérios cumulativos. A natureza da informação é o primeiro elemento: fatos verificáveis demandam compromisso com veracidade mínima, enquanto opiniões admitem maior margem valorativa. Ainda assim, opiniões não podem servir como disfarce para ataques discriminatórios ou humilhações deliberadas (Tartuce, 2025).

O interesse público também é relevante. Informações sobre atuação profissional, práticas comerciais, condutas de agentes públicos ou riscos coletivos podem justificar maior grau de exposição. Já dados íntimos sem relevância social, ainda que verdadeiros, podem configurar violação à privacidade quando divulgados apenas para constranger (Schreiber, 2021).

A forma de manifestação deve ser considerada. Linguagem agressiva, montagem vexatória, ameaça, insulto reiterado, exposição de familiares, uso de perfis falsos ou convocação de ataques indicam abuso. A crítica legítima pode ser dura, mas não deve converter-se em instrumento de aniquilação moral (Gagliano; Pamplona Filho, 2026).

A escala de difusão e a persistência também importam. Uma crítica isolada em ambiente restrito tem impacto diferente de campanha viral com milhares de compartilhamentos, impulsionamento, hashtags e repostagens continuadas. O alcance não é mero detalhe, mas elemento da extensão do dano (Tartuce, 2025).

4.3 CANCELAMENTO DIGITAL E CAUSALIDADE EM REDE

O cancelamento digital pode ser entendido como dinâmica coletiva de reprovação pública que, em determinados casos, ultrapassa a crítica e se converte em processo de exclusão, estigmatização e destruição reputacional. Nem todo boicote ou crítica coletiva é ilícito, mas a coordenação desproporcional de ataques pode violar direitos da personalidade (Schreiber, 2021).

A causalidade em casos de cancelamento é complexa porque o dano resulta de múltiplas interações. Um primeiro conteúdo pode desencadear comentários, memes, republicações, vídeos, notícias, perdas comerciais e isolamento social. A responsabilidade civil precisa identificar contribuições relevantes sem punir automaticamente todos os participantes da rede (Tartuce, 2025).

A participação relevante pode ocorrer quando o agente cria conteúdo falso, impulsiona conscientemente ofensa, convoca ataques, divulga dados pessoais, ameaça, insiste após esclarecimentos ou explora economicamente a exposição. Nesses casos, há contribuição causal qualificada para a intensificação do dano (Gagliano; Pamplona Filho, 2026).

A mera discordância, curtida ou compartilhamento sem consciência do conteúdo ilícito deve ser tratada com cautela. A responsabilização excessiva pode gerar efeito inibidor sobre a liberdade de expressão. Por isso, a análise deve separar adesão banal ao debate de participação ativa na cadeia de lesão (Vieira, 2019).

As plataformas também influenciam a dinâmica do dano. Algoritmos de recomendação, métricas de engajamento e monetização podem ampliar conteúdos ofensivos. Embora o Marco Civil estabeleça regime específico para responsabilidade de provedores por conteúdo de terceiros, a omissão diante de conteúdos manifestamente ilícitos ou reiteradamente denunciados pode ser relevante na avaliação do dever de cuidado (Leonardi, 2019).

A quantificação do dano moral digital deve considerar elementos específicos: alcance da publicação, tempo de exposição, grau de replicação, conteúdo ofensivo, posição social da vítima, vulnerabilidade, consequências demonstráveis e conduta posterior do ofensor. Essa metodologia evita arbitrariedade e aproxima a reparação da extensão real da lesão (Tartuce, 2025).

4.4 PROVA DIGITAL E EFETIVIDADE DA TUTELA

A prova do dano digital apresenta dificuldades próprias. Conteúdos podem ser apagados, perfis podem ser excluídos, autores podem usar anonimato, links podem desaparecer e plataformas podem limitar acesso a dados. A volatilidade da informação exige atuação rápida da vítima e do Poder Judiciário (Schreiber, 2021).

A ata notarial, os registros de URL, prints contextualizados, metadados, relatórios de plataforma, testemunhas, perícia técnica e preservação de logs podem ser instrumentos relevantes. A prova deve buscar demonstrar não apenas a existência da publicação, mas também sua autoria, alcance, persistência e relação com o dano alegado (Leonardi, 2019).

A preservação de registros deve compatibilizar proteção da vítima, privacidade de terceiros e devido processo. O Marco Civil da Internet disciplina guarda e fornecimento de registros em hipóteses específicas, exigindo ordem judicial para acesso a determinados dados. Essa estrutura busca equilibrar investigação de ilícitos e proteção de direitos fundamentais (Leonardi, 2019).

A tutela de urgência pode ser necessária para remoção de conteúdo, preservação de provas, suspensão de divulgação e identificação de responsáveis. Contudo, deve ser manejada com proporcionalidade, especialmente quando houver discussão sobre interesse público e liberdade de expressão (Vieira, 2019).

A efetividade da responsabilidade civil digital depende, portanto, de instrumentos processuais adequados e de compreensão técnica mínima pelos operadores do Direito. Sem prova preservada e critérios de análise coerentes, a vítima pode permanecer desprotegida ou o réu pode ser responsabilizado de forma excessiva (Gagliano; Pamplona Filho, 2026).

5 DECISÕES ALGORÍTMICAS E NOVOS LIMITES DA RESPONSABILIDADE CIVIL

5.1 OPACIDADE, AUTONOMIA RELATIVA E IMPREVISIBILIDADE

As decisões algorítmicas diferem das decisões humanas tradicionais porque resultam de modelos computacionais que processam dados e produzem resultados a partir de regras, padrões estatísticos ou aprendizado de máquina. Em sistemas mais simples, a lógica é previsível; em sistemas complexos, especialmente aqueles baseados em aprendizado profundo, a explicação do resultado pode ser difícil até para desenvolvedores (Calo, 2017).

A opacidade técnica é frequentemente descrita como problema de caixa-preta. O usuário afetado conhece o resultado, mas não compreende a trajetória decisória. Essa opacidade dificulta a impugnação, a prova do defeito e a identificação do responsável. Quando o sistema nega crédito, bloqueia conta, classifica risco ou recomenda medida automatizada, a ausência de explicação compromete a tutela civil (Floridi, 2021).

A autonomia da inteligência artificial é relativa, pois sistemas dependem de dados, objetivos, arquitetura e parâmetros definidos por humanos. Ainda assim, seus resultados podem não ser plenamente previsíveis, especialmente quando modelos aprendem padrões ocultos, reproduzem vieses ou interagem com ambientes dinâmicos. Essa imprevisibilidade tensiona a responsabilidade baseada em culpa (Tepedino; Silva, 2020).

O dano algorítmico pode decorrer de múltiplas fontes: base de dados enviesada, programação defeituosa, ausência de auditoria, uso fora do contexto, falha de supervisão, treinamento inadequado, erro de integração ou decisão empresarial de automatizar etapa sensível. A causalidade, portanto, não é linear, mas distribuída entre vários agentes técnicos e econômicos (Teffé; Medon, 2020).

A responsabilidade civil deve considerar quem criou o sistema, quem o treinou, quem forneceu dados, quem definiu a finalidade, quem implementou a ferramenta e quem se beneficiou da decisão. A mera alegação de que a máquina decidiu não pode afastar o dever de reparar, pois sistemas automatizados são colocados em operação por escolhas humanas e empresariais (Calo, 2017).

A opacidade não deve funcionar como privilégio do fornecedor tecnológico. Pelo contrário, quanto mais difícil for para a vítima compreender o processo decisório, maior deve ser o dever de documentação, explicação e prova por parte de quem controla o sistema. Essa inversão funcional preserva a efetividade da responsabilidade civil (Floridi, 2021).

5.2 TRANSPARÊNCIA, EXPLICABILIDADE E AUDITORIA

A transparência em sistemas algorítmicos não significa revelar integralmente segredos industriais ou códigos-fonte em qualquer situação. Significa fornecer informações suficientes para que usuários, autoridades e vítimas compreendam a lógica geral do sistema, seus critérios relevantes, suas limitações e seus impactos potenciais (Floridi, 2021).

A explicabilidade é mais específica. Ela busca permitir que a pessoa afetada entenda por que determinado resultado foi produzido. Em decisões que afetam direitos, crédito, trabalho, acesso a serviços, reputação ou patrimônio, a explicação não pode ser meramente formal. Deve ser útil para contestação, revisão e eventual responsabilização (Calo, 2017).

A auditoria independente constitui mecanismo de controle essencial. Sistemas de IA podem produzir discriminação, erro, exclusão injustificada ou tratamento desigual sem que isso seja evidente na interface. Auditorias de dados, de modelo e de resultado permitem identificar vieses, falhas de segurança, inconsistências e danos sistêmicos (Floridi, 2021).

A rastreabilidade também é fundamental. Decisões algorítmicas relevantes devem deixar registros mínimos sobre dados utilizados, parâmetros aplicados, versões do sistema, revisões humanas e alterações posteriores. Sem trilha de auditoria, a vítima dificilmente conseguirá reconstruir o nexo causal (Teffé; Medon, 2020).

A supervisão humana deve ser efetiva, e não apenas simbólica. O controlador não cumpre seu dever se coloca um agente humano incapaz de revisar criticamente o resultado automatizado. Supervisão pressupõe competência técnica, autoridade para alterar a decisão e responsabilidade pelo uso do sistema (Tepedino; Silva, 2020).

Esses deveres convergem com a abordagem regulatória baseada em risco. Quanto maior o potencial de dano do sistema, maior deve ser o grau de transparência, documentação, supervisão e responsabilização. Essa lógica aparece tanto em debates brasileiros sobre regulação de IA quanto no modelo europeu de inteligência artificial (Floridi, 2021).

5.3 RESPONSABILIDADE CIVIL E REGULAÇÃO DE INTELIGÊNCIA ARTIFICIAL

O Projeto de Lei nº 2.338/2023 representa tentativa brasileira de estruturar normas gerais para desenvolvimento, implementação e uso responsável de sistemas de inteligência artificial. Sua orientação geral dialoga com princípios como centralidade da pessoa humana, transparência, segurança, não discriminação, responsabilização e prevenção de danos (Brasil, 2023).

A regulação da IA deve complementar, e não substituir, os regimes já existentes de responsabilidade civil, consumidor, proteção de dados e direitos fundamentais. Danos algorítmicos podem envolver simultaneamente defeito do serviço, tratamento indevido de dados, discriminação, publicidade abusiva e violação de direitos da personalidade (Doneda; Mendes, 2024).

O AI Act europeu adota abordagem baseada em risco, impondo obrigações mais intensas a sistemas classificados como de alto risco. Embora pertença a outro ordenamento, o modelo oferece referência importante para o debate brasileiro ao diferenciar obrigações conforme potencial lesivo e contexto de aplicação da tecnologia (Floridi, 2021).

A responsabilidade civil em matéria algorítmica deve ser híbrida. Em sistemas de alto risco ou em atividades de consumo, a responsabilidade objetiva tende a ser mais adequada. Em sistemas de menor risco, pode-se admitir análise mais próxima da culpa, mas com deveres reforçados de informação, documentação e cooperação probatória (Teffé; Medon, 2020).

A prevenção deve ocupar papel central. A reparação posterior pode ser insuficiente quando o dano algorítmico atinge milhares de consumidores, bloqueia acesso a serviços essenciais ou reproduz discriminação estrutural. Por isso, medidas de governança, avaliação de impacto, auditoria e segurança devem preceder a implantação do sistema (Calo, 2017).

O Direito Civil não pode tratar a IA como fenômeno excepcional ou futurista. Ela já está inserida em atividades ordinárias. A função da responsabilidade civil é assegurar que a inovação não reduza o nível de proteção da pessoa, do consumidor e dos direitos fundamentais (Tepedino; Silva, 2020).

6 PARÂMETROS PARA UMA RESPONSABILIDADE CIVIL DIGITAL

6.1 CRITÉRIOS DE IMPUTAÇÃO NAS FRAUDES DIGITAIS

A responsabilidade em fraudes digitais deve partir da identificação do risco criado ou controlado. Quando o dano decorre de falha previsível do serviço, ausência de monitoramento, deficiência de informação ou vulnerabilidade estrutural, a imputação deve recair sobre o fornecedor ou cadeia de fornecedores que exploram economicamente a atividade (Miragem, 2024).

O segundo critério é a capacidade de prevenção. Deve responder prioritariamente quem possui melhores condições técnicas e econômicas de evitar o dano. Bancos podem monitorar transações; marketplaces podem verificar vendedores; gateways podem detectar operações suspeitas; plataformas podem estruturar denúncia e remoção; influenciadores podem informar patrocínio e riscos (Marques, 2023).

O terceiro critério é a confiança induzida. Quem se apresenta como ambiente seguro, intermediador confiável ou especialista em prevenção assume deveres proporcionais à confiança que desperta. O consumidor não contrata apenas produto ou serviço, mas também segurança, reputação e assistência em caso de problema (Cavalieri Filho, 2023).

O quarto critério é a resposta ao incidente. Mesmo quando a fraude não era totalmente evitável, a demora em bloquear conta, contestar operação, preservar provas ou orientar a vítima pode agravar o

dano e gerar responsabilidade. A conduta posterior do fornecedor integra a análise do defeito do serviço (Doneda; Mendes, 2024).

Esses critérios permitem distinguir hipóteses de fortuito interno e externo. O fortuito externo deve ser reservado a eventos completamente estranhos à atividade e inevitáveis, enquanto o fortuito interno abrange fraudes, falhas, ataques e riscos previsíveis do serviço digital (Schreiber, 2025).

6.2 CRITÉRIOS PARA O DANO MORAL DIGITAL

A aferição do dano moral digital deve considerar a natureza do conteúdo. Acusações falsas, exposição de intimidade, divulgação de dados sensíveis, discurso discriminatório e imputações criminosas possuem maior potencial lesivo do que críticas genéricas ou opiniões desagradáveis (Schreiber, 2021).

O interesse público deve funcionar como fator de ponderação. Informações relevantes para proteção de consumidores, fiscalização de autoridades, debate político ou denúncia de irregularidades merecem maior proteção, desde que divulgadas com responsabilidade e sem abuso manifesto (Vieira, 2019).

A forma de manifestação deve ser examinada. A crítica civilmente lícita pode ser firme; entretanto, insultos reiterados, montagens humilhantes, perseguição, ameaças e exposição de familiares indicam desvio de finalidade e abuso do direito (Tartuce, 2025).

A escala e a persistência são critérios próprios da era digital. O número de visualizações, compartilhamentos, republicações, tempo de permanência online e indexação por buscadores pode ampliar a extensão do dano. A reparação deve considerar essa dimensão material da circulação (Schreiber, 2021).

O dano verificável também importa. Perda de contrato, afastamento profissional, sofrimento psíquico demonstrado, necessidade de tratamento, ameaça concreta, bloqueio social e repercussão econômica são elementos que ajudam a mensurar a gravidade, sem exigir prova impossível em situações de exposição evidente (Gagliano; Pamplona Filho, 2026).

6.3 CRITÉRIOS PARA DECISÕES ALGORÍTMICAS

Nas decisões algorítmicas, o primeiro critério é o grau de impacto sobre direitos. Sistemas que afetam crédito, trabalho, consumo, saúde, educação, segurança, acesso a serviços e reputação exigem maior controle. Quanto mais relevante o impacto, maior deve ser a exigência de explicabilidade e revisão humana (Floridi, 2021).

O segundo critério é o grau de autonomia. Sistemas meramente auxiliares, que apenas organizam dados para decisão humana, produzem riscos diferentes de sistemas que bloqueiam, negam,

aprovam ou recomendam automaticamente sem revisão efetiva. A imputação deve acompanhar o nível de automatização (Calo, 2017).

O terceiro critério é a governança de dados. Bases desatualizadas, enviesadas, incompletas ou coletadas sem fundamento adequado aumentam a probabilidade de dano. A qualidade dos dados é elemento jurídico relevante, porque decisões automatizadas dependem diretamente da informação processada (Doneda; Mendes, 2024).

O quarto critério é a documentação do sistema. Sem registros sobre versão, parâmetros, dados e intervenção humana, a vítima fica impossibilitada de demonstrar a falha. A ausência de documentação deve pesar contra quem controla a tecnologia, sobretudo em relações de consumo (Teffé; Medon, 2020).

O quinto critério é a auditabilidade. Sistemas de alto impacto devem ser passíveis de avaliação independente, de modo que erros sistêmicos, discriminação e falhas de desempenho possam ser identificados. A auditoria transforma a responsabilidade civil de mecanismo meramente reativo em instrumento de prevenção (Floridi, 2021).

6.4 PROPOSTA DE SÍNTESE

A responsabilidade civil digital deve ser construída sobre quatro pilares: risco, segurança, transparência e proporcionalidade. O risco permite atribuir responsabilidade a quem explora atividade perigosa ou vulnerável; a segurança define deveres preventivos; a transparência viabiliza prova e controle; a proporcionalidade impede censura, excesso indenizatório ou inibição injustificada da inovação (Tartuce, 2025).

Esses pilares devem dialogar com os regimes normativos já existentes. O Código Civil fornece a base geral da reparação; o Código de Defesa do Consumidor estabelece responsabilidade objetiva e solidariedade; o Marco Civil da Internet regula aspectos de provedores e registros; a LGPD impõe governança de dados; e a futura regulação de IA pode complementar deveres de explicabilidade e auditoria (Doneda; Mendes, 2024).

A vítima deve ocupar posição central. A complexidade técnica não pode justificar desproteção. Se o agente econômico cria ambiente digital, coleta dados, automatiza decisões e lucra com escala, deve assumir deveres proporcionais de prevenção e reparação. A inovação tecnológica só é socialmente legítima quando acompanhada de responsabilidade (Schreiber, 2025).

Por outro lado, a responsabilidade civil não deve impedir todo risco. O ambiente digital envolve incertezas e transformações contínuas. A função do Direito é organizar riscos, impor deveres razoáveis e reparar danos injustos, sem inviabilizar atividades úteis. O equilíbrio entre inovação e proteção depende de critérios claros e aplicação prudente (Floridi, 2021).

7 CONCLUSÃO

O presente estudo analisou a responsabilidade civil na era digital a partir de três frentes interligadas: fraudes eletrônicas nas relações de consumo, dano moral em ambientes virtuais e decisões algorítmicas. A pesquisa demonstrou que os pressupostos clássicos da responsabilidade civil continuam relevantes, mas precisam ser reinterpretados diante da complexidade tecnológica, da multiplicidade de agentes e da amplificação dos danos em rede.

No campo das fraudes digitais, verificou-se que a responsabilidade objetiva fundada no risco do empreendimento e no dever de segurança deve ocupar posição central. Bancos, marketplaces, gateways, empresas antifraude, transportadoras, anunciantes e influenciadores digitais podem integrar a cadeia de fornecimento quando participam da operação, induzem confiança, lucram com a intermediação ou possuem capacidade de prevenir o dano.

A distinção entre fortuito interno e fortuito externo permanece essencial. Fraudes previsíveis no ambiente digital, especialmente quando relacionadas à atividade econômica explorada, devem ser tratadas como fortuito interno, não afastando a responsabilidade do fornecedor. A culpa exclusiva da vítima deve ser reconhecida apenas em hipóteses excepcionais e mediante prova robusta, sob pena de transferir ao consumidor o risco estrutural da digitalização.

Quanto ao dano moral digital, constatou-se que a lesão aos direitos da personalidade não decorre apenas do conteúdo originário da manifestação, mas também da forma como esse conteúdo circula, permanece, é replicado e produz exposição pública continuada. A viralização, a persistência e a escala de difusão são elementos constitutivos da extensão do dano.

A distinção entre crítica legítima e ilícito civil indenizável exige critérios cumulativos. Devem ser considerados a natureza da informação, o interesse público, a forma de manifestação, a escala de difusão, a persistência do conteúdo, a existência de dano verificável e a contribuição causal de cada agente. Essa metodologia permite proteger a honra, a imagem e a privacidade sem restringir indevidamente a liberdade de expressão.

No campo das decisões algorítmicas, observou-se que a opacidade, a autonomia relativa e a imprevisibilidade dos sistemas desafiam o modelo tradicional de culpa e causalidade linear. A responsabilidade civil precisa incorporar transparência, explicabilidade, rastreabilidade, auditoria e supervisão humana como deveres jurídicos relevantes, especialmente em sistemas de alto impacto.

A ausência de explicação não pode beneficiar quem controla a tecnologia. Quando a vítima não consegue compreender a decisão automatizada, cabe ao fornecedor, controlador ou operador demonstrar a adequação do sistema, a qualidade dos dados, a inexistência de defeito e a adoção de medidas preventivas. A complexidade técnica deve gerar maior dever de documentação, não menor responsabilidade.

A pesquisa também evidenciou que a tutela civil digital deve dialogar com diferentes regimes normativos. Código Civil, Código de Defesa do Consumidor, Marco Civil da Internet, LGPD e futura regulação de IA devem ser interpretados de forma sistemática, pois os danos digitais raramente se enquadram em apenas uma categoria jurídica.

Conclui-se que a responsabilidade civil na era digital deve abandonar respostas simplistas. Nem toda falha tecnológica gera indenização automática, mas também não se pode exigir da vítima prova impossível sobre sistemas opacos, cadeias complexas e riscos controlados por agentes econômicos. O caminho mais adequado está em uma responsabilidade funcional, preventiva e proporcional, capaz de distribuir riscos conforme controle, benefício econômico, capacidade de prevenção e proteção dos direitos fundamentais.

Por fim, recomenda-se que futuras pesquisas aprofundem a análise empírica da jurisprudência brasileira sobre fraudes digitais, cancelamento online e decisões automatizadas, especialmente quanto aos critérios de quantificação do dano moral, à responsabilidade de plataformas ativas e aos efeitos da futura regulação brasileira de inteligência artificial. A consolidação de parâmetros objetivos será indispensável para garantir segurança jurídica, confiança digital e efetividade da tutela civil.

REFERÊNCIAS

BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. São Paulo: Thomson Reuters Brasil, 2018.

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: 8 jun. 2026.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Código de Defesa do Consumidor. Brasília, DF: Presidência da República, 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 8 jun. 2026.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Código Civil. Brasília, DF: Presidência da República, 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 8 jun. 2026.

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: 8 jun. 2026.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 8 jun. 2026.

BRASIL. Senado Federal. Projeto de Lei nº 2.338, de 2023. Dispõe sobre o uso da inteligência artificial. Brasília, DF: Senado Federal, 2023. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/157233. Acesso em: 8 jun. 2026.

CALO, Ryan. Artificial intelligence policy: a primer and roadmap. University of California, Davis Law Review, Davis, v. 51, p. 399-435, 2017.

CAVALIERI FILHO, Sergio. Programa de responsabilidade civil. 16. ed. Barueri: Atlas, 2023.

DINIZ, Maria Helena. Curso de direito civil brasileiro: responsabilidade civil. 33. ed. São Paulo: Saraiva, 2019. v. 7.

DONEDA, Danilo; MENDES, Laura Schertel. Comentários à Lei Geral de Proteção de Dados. 3. ed. São Paulo: SaraivaJur, 2024.

EUROPEAN UNION. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence. Official Journal of the European Union, 2024. Disponível em: https://eur-lex.europa.eu/. Acesso em: 8 jun. 2026.

FLORIDI, Luciano. The fourth revolution: how the infosphere is reshaping human reality. Oxford: Oxford University Press, 2014.

FLORIDI, Luciano. The end of an era: from self-regulation to hard law for the digital industry. Philosophy & Technology, Dordrecht, v. 34, p. 619-622, 2021.

GAGLIANO, Pablo Stolze; PAMPLONA FILHO, Rodolfo. Novo curso de direito civil: responsabilidade civil. 24. ed. São Paulo: SaraivaJur, 2026. v. 3.

GONÇALVES, Carlos Roberto. Responsabilidade civil. 18. ed. São Paulo: Saraiva, 2019.

LEONARDI, Marcel. Responsabilidade civil dos provedores de serviços de internet. São Paulo: Juarez de Oliveira, 2019.

MARQUES, Cláudia Lima. Contratos no Código de Defesa do Consumidor. 12. ed. São Paulo: Revista dos Tribunais, 2023.

MIRAGEM, Bruno. Curso de direito do consumidor. 16. ed. São Paulo: Revista dos Tribunais, 2024.

SCHREIBER, Anderson. Direitos da personalidade. São Paulo: Atlas, 2021.

SCHREIBER, Anderson. Responsabilidade civil digital. 2. ed. Rio de Janeiro: Forense, 2025.

SUPERIOR TRIBUNAL DE JUSTIÇA. Súmula nº 479. As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias. Brasília, DF: STJ, 2012.

TARTUCE, Flávio. Responsabilidade civil. 6. ed. Rio de Janeiro: Forense, 2025.

TEFFE, Chiara Spadaccini de; MEDON, Filipe. Responsabilidade civil e regulação de novas tecnologias: questões acerca da utilização de inteligência artificial na tomada de decisões empresariais. Revista Estudos Institucionais, Rio de Janeiro, v. 6, n. 1, p. 301-333, 2020.

TEPEDINO, Gustavo; SILVA, Rodrigo da Guia. O Direito Civil na era da inteligência artificial. São Paulo: Thomson Reuters Brasil, 2020.

VIEIRA, Oscar Vilhena. Direitos fundamentais: uma leitura da jurisprudência do STF. 2. ed. São Paulo: Malheiros, 2019.