

Responsabilidade Civil na Sociedade Contemporânea: Novos Desafios Diante das Relações Digitais

Civil Liability In Contemporary Society: New Challenges In Digital Relations

*Responsabilidad Civil En La Sociedad Contemporánea: Nuevos Desafíos Ante
Las Relaciones Digitale*

 <https://doi.org/10.5281/zenodo.22978963>

Recebido: 21 de setembro de 2026

Aceito: 24 de setembro de 2026

Publicado: 26 de setembro de 2026

Ingrid Costa Cardoso

Mestra em profissional em Educação
Universidade Regional do Cariri (URCA)

✉ ingridcardosoadv@gmail.com

 <http://lattes.cnpq.br/1828188355435441>

Luciano Alves Daniel

Especialização em Curso de Especialização Direito de Processo Penal
Centro Universitário Dr. Leão Sampaio (UNILEAO)

✉ luciano.a.daniel.adv@gmail.com

 <http://lattes.cnpq.br/8687515882597429>

Jesus de Souza Cartaxo

Doutor em Ciências da Saúde
Faculdade de Medicina do ABC (FMABC)

✉ jcartaxoadv@gmail.com

 <http://lattes.cnpq.br/5535720585940084>

Eliane da Silva Ferreira Moura

Mestra em profissional em Educação Profissional e Tecnológica
Instituto Federal do Sertão Pernambucano, IF-Sertão

✉ elianedasilvaferreiramoura@gmail.com

 <http://lattes.cnpq.br/4482421373414153>

Sayron Rilley Carmo Bezerra

Mestre em profissional em Educação
Universidade Regional do Cariri (URCA)

✉ sayronrilleycarmobezerra@gmail.com

 <http://lattes.cnpq.br/6846181600408970>

 <https://orcid.org/0000-0001-7801-0055>

Teresa Maria Siqueira Nascimento Arrais

Mestra em profissional em Educação Profissional

Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte (IFRN)

✉ teresasiqueira.ts@gmail.com

🌐 <http://lattes.cnpq.br/7934349347164073>

Maria Conceição Santos Sales

Especialização em Psicologia Jurídica e Avaliação Psicológica

Faculdade Venda Nova do Imigrante (FAVENI)

✉ psisalesmaria@outlook.com

🌐 <http://lattes.cnpq.br/3699937462536152>

Cristóvão Maia Filho

Mestrado em Educação Profissional e Tecnológica

Instituto Federal de Pernambuco Sertão (IFSERTÃOPE)

✉ cristovaomaia72@gmail.com

🌐 <http://lattes.cnpq.br/7766897607760493>

🆔 <https://orcid.org/0000-0003-3605-5743>

Resumo: A digitalização das relações sociais e econômicas transferiu parte expressiva das interações privadas para ambientes mediados por plataformas, dados, algoritmos e contratos eletrônicos, produzindo novas formas de dano e desafios à responsabilidade civil. Este artigo analisa esses desafios, com ênfase em plataformas digitais, proteção de dados pessoais, comércio eletrônico e inteligência artificial. Realizou-se revisão narrativa estruturada de artigos científicos indexados na SciELO, publicados entre 2000 e 2026 e selecionados por pertinência ao problema jurídico investigado. O corpus reuniu dezesseis estudos com identificação bibliográfica e DOI ou registro editorial verificável. A literatura indica que o ambiente digital não elimina as categorias clássicas de conduta, dano e nexos causal, mas exige sua releitura diante da opacidade algorítmica, assimetria informacional, tratamento massivo de dados e intermediação por plataformas. Observa-se também maior ênfase em deveres de prevenção, segurança, informação, transparência e governança. Conclui-se que a responsabilidade civil contemporânea deve combinar fundamentos tradicionais do direito privado com parâmetros de diligência compatíveis com riscos tecnológicos, preservando inovação sem reduzir a tutela da personalidade, da privacidade e da confiança.

Palavras-chave: responsabilidade civil; relações digitais; plataformas digitais; proteção de dados; inteligência artificial.

Abstract: The digitalization of social and economic relations has shifted a substantial share of private interactions to environments mediated by platforms, data, algorithms, and electronic contracts, creating new forms of harm and challenges for civil liability. This article analyzes these challenges, focusing on digital platforms, personal data protection, e-commerce, and artificial intelligence. A structured narrative review was conducted of scientific articles indexed in SciELO, published between 2000 and 2026 and selected for direct relevance to the legal problem investigated. The final corpus comprised sixteen studies with verifiable bibliographic identification and DOI or editorial record. The literature indicates that the digital environment does not eliminate the classic categories of conduct, damage, and causation, but requires their reinterpretation in light of algorithmic opacity, information asymmetry, large-scale data processing, and platform intermediation. Greater emphasis is also placed on duties of prevention, security, information, transparency, and governance. Contemporary civil liability should therefore combine traditional private-law foundations with standards of diligence suited to technological risks, preserving innovation without weakening the protection of personality, privacy, and trust.

Keywords: civil liability; digital relations; digital platforms; data protection; artificial intelligence.

Resumen: La digitalización de las relaciones sociales y económicas trasladó una parte sustancial de las interacciones privadas a entornos mediados por plataformas, datos, algoritmos y contratos electrónicos, generando nuevas formas de daño y desafíos para la responsabilidad civil. Este artículo analiza esos desafíos, con énfasis en plataformas digitales, protección de datos personales, comercio electrónico e inteligencia artificial. Se realizó una revisión narrativa estructurada de artículos científicos indexados en SciELO, publicados entre 2000 y 2026 y seleccionados por su pertinencia directa al problema jurídico investigado. El corpus final reunió dieciséis estudios con identificación bibliográfica y DOI o registro editorial verificable. La literatura indica que el entorno

digital no elimina las categorías clásicas de conducta, daño y nexo causal, pero exige reinterpretarlas ante la opacidad algorítmica, la asimetría informacional, el tratamiento masivo de datos y la intermediación de plataformas. También aumenta la importancia de los deberes de prevención, seguridad, información, transparencia y gobernanza. Se concluye que la responsabilidad civil contemporánea debe combinar los fundamentos tradicionales del derecho privado con estándares de diligencia compatibles con los riesgos tecnológicos, preservando la innovación sin debilitar la tutela de la personalidad, la privacidad y la confianza.

Palabras clave: responsabilidad civil; relaciones digitales; plataformas digitales; protección de datos; inteligencia artificial.

1. INTRODUÇÃO

A responsabilidade civil sempre ocupou posição central no direito privado por funcionar como técnica de recomposição de danos e, simultaneamente, como mecanismo de organização de expectativas sociais. Em sua formulação clássica, a análise jurídica procura identificar uma conduta juridicamente relevante, um dano, um nexo causal e, conforme o regime aplicável, a culpa ou outro fator de atribuição. A expansão das tecnologias digitais não tornou essas categorias inúteis, mas alterou profundamente o contexto em que elas operam. Hoje, relações contratuais podem ser formadas sem presença física, danos podem adquirir alcance massivo em poucos segundos, decisões podem ser automatizadas e intermediários privados exercem funções relevantes na circulação de informações, na organização de mercados e na seleção de conteúdos. A consequência é um cenário em que a imputação jurídica depende, cada vez mais, da compreensão da arquitetura tecnológica e da distribuição concreta de poder entre usuários, empresas e plataformas.

Os estudos sobre contratos eletrônicos já demonstravam, desde o início da consolidação do comércio digital, que a forma tecnológica da contratação modifica problemas de formação, prova, segurança e confiança, sem extinguir a lógica jurídica do vínculo obrigacional. Forgioni (2000) discutiu a tensão entre celeridade econômica e proteção do consumidor no comércio eletrônico, enquanto Barreto (2009) descreveu o contrato eletrônico como estrutura híbrida entre sistemas sociais e ambientes digitais. Posteriormente, Polido e Silva (2017) mostraram que a transnacionalidade das contratações eletrônicas amplia dificuldades relativas à lei aplicável, à validade do negócio e à segurança jurídica. Esses trabalhos indicam que a transformação digital não se limita à mudança do suporte documental: ela modifica a própria forma de circulação de riscos e informações.

Com a consolidação das plataformas digitais, a discussão tornou-se ainda mais complexa. A plataforma não atua apenas como espaço neutro de encontro, pois seus sistemas de classificação, recomendação, moderação, monetização e desenho de interfaces podem influenciar o comportamento dos usuários e a visibilidade dos conteúdos. Brega (2023) examina a responsabilidade por conteúdos publicados em redes sociais e mostra que a

regulação brasileira foi construída em torno de um delicado equilíbrio entre liberdade de expressão, deveres dos provedores e retirada de conteúdos. Já Lemos e Estima (2026), ao analisarem o julgamento dos temas de repercussão geral relacionados ao artigo 19 do Marco Civil da Internet, destacam a crescente relevância jurídica da própria materialidade das plataformas e de seus mecanismos algorítmicos para a atribuição de responsabilidade.

Outro vetor de transformação é a centralidade econômica dos dados pessoais. Boff e Fortes (2014) já apontavam a necessidade de reconhecer a privacidade e a proteção de dados no ciberespaço como direitos fundamentais. Szinvelski, Arceno e Francisco (2019) demonstraram que o avanço do big data intensifica o compartilhamento, a inferência e o tratamento de informações, exigindo do Direito uma função protetiva capaz de limitar usos incompatíveis com a autonomia do titular. Em perspectiva crítica, Fornasier e Knebel (2021) associam o tratamento de dados à economia de vigilância e ressaltam a assimetria estrutural entre usuários e agentes capazes de coletar, processar e monetizar grandes volumes de informação. A transformação do dado em recurso econômico faz surgir danos que nem sempre se manifestam como perda patrimonial imediata, mas como exposição, perda de controle informacional, perfilamento abusivo e redução da autonomia decisória.

A inteligência artificial adiciona outra camada de dificuldade ao problema. Barroso e Mello (2024) identificam riscos decorrentes de sistemas capazes de automatizar decisões e operar em ambientes nos quais explicabilidade, supervisão humana, segurança e responsabilidade se tornam requisitos essenciais. Santos e Graminho (2024), ao tratarem da discriminação algorítmica, evidenciam que a automação pode reproduzir ou ampliar assimetrias e vieses, de modo que o dano pode resultar da combinação entre dados de entrada, modelos estatísticos, decisões de implementação e ausência de controle institucional. Nesse contexto, a pergunta sobre “quem causou o dano” deixa de ser respondida apenas pela observação de um ato individual e passa a exigir a reconstrução de uma cadeia de escolhas técnicas e organizacionais.

Essas mudanças não significam que toda inovação tecnológica deva gerar presunção de responsabilidade ou que a simples ocorrência de um resultado adverso seja suficiente para impor dever de indenizar. O desafio consiste em adaptar critérios jurídicos de diligência e imputação sem transformar a responsabilidade civil em instrumento de bloqueio tecnológico. A literatura recente sobre plataformas digitais mostra que a regulação eficiente precisa considerar, ao mesmo tempo, capacidade técnica, previsibilidade, poder de controle, grau de intervenção na atividade e deveres de transparência. Gonçalves, Coutinho e Kira (2022) e

Barros e Prol (2025) evidenciam que as plataformas concentram poder econômico e regulatório significativo, razão pela qual a análise jurídica não pode ignorar a dimensão institucional dos modelos de negócio digitais.

A relevância do tema é ampliada porque os danos digitais tendem a combinar características distintas: rapidez de propagação, persistência, replicabilidade, dificuldade de reversão, atuação transfronteiriça e potencial afetação simultânea de grande número de pessoas. A proteção jurídica, portanto, precisa dialogar com direitos da personalidade, relações de consumo, obrigações contratuais, proteção de dados e deveres específicos de intermediários. Tomasevicius Filho (2016) já observava que os problemas da internet alcançam privacidade, honra e imagem, enquanto a literatura mais recente desloca o foco para deveres sistêmicos de segurança, governança e prevenção. A questão central não é criar uma responsabilidade civil completamente nova, mas compreender como seus fundamentos respondem a um ambiente em que os riscos são distribuídos por redes técnicas e empresariais.

Diante desse quadro, o problema de pesquisa consiste em identificar quais são os principais desafios que as relações digitais impõem à responsabilidade civil contemporânea e de que modo a produção científica indexada tem reinterpretado categorias como dano, nexo causal, culpa, risco, dever de cuidado e prevenção. A hipótese sustentada é que a resposta jurídica mais consistente não reside em abandonar as categorias clássicas, mas em complementá-las com deveres de diligência tecnológica, transparência, segurança, governança e proteção da confiança, calibrados conforme o grau de controle e intervenção do agente sobre o risco.

O objetivo geral é analisar os desafios contemporâneos da responsabilidade civil decorrentes da digitalização das relações privadas, considerando a atuação de plataformas, o tratamento de dados pessoais, a contratação eletrônica e o uso de sistemas algorítmicos. Pretende-se compreender de que forma a literatura científica recente tem adaptado ou problematizado os elementos tradicionais da responsabilidade civil diante de novas estruturas de intermediação e decisão.

Como objetivos específicos, busca-se: a) examinar a transformação dos deveres de cuidado e informação em ambientes digitais; b) identificar os principais problemas de imputação relacionados às plataformas e aos conteúdos de terceiros; c) discutir como privacidade, proteção de dados e perfilamento alteram a compreensão do dano; d) analisar as repercussões da automação e da inteligência artificial sobre causalidade, previsibilidade e atribuição; e e) sintetizar critérios jurídicos capazes de orientar uma responsabilidade civil

compatível com inovação, prevenção e tutela efetiva dos direitos da personalidade.

2. REFERENCIAL TEÓRICO

2.1 A digitalização das relações privadas e a permanência das categorias clássicas

A literatura analisada mostra que a digitalização não rompeu com a estrutura fundamental da responsabilidade civil, mas tornou mais difícil a reconstrução dos fatos juridicamente relevantes. No ambiente analógico, a identificação do agente, da conduta e do resultado costuma ser favorecida por uma cadeia causal mais visível. Nas relações digitais, uma mesma consequência pode decorrer da combinação entre comportamento do usuário, regras contratuais, desenho da interface, tratamento automatizado de informações, falhas de segurança e decisões empresariais. A imputação, portanto, tende a depender menos da busca por um único ato isolado e mais da compreensão do processo que produziu o dano.

Os estudos pioneiros sobre comércio eletrônico já demonstravam essa mudança. Forgioni (2000) examinou a formação e a prova dos contratos eletrônicos em um contexto no qual segurança e velocidade precisavam ser conciliadas com proteção do consumidor. Barreto (2009) aprofundou a discussão ao caracterizar o contrato eletrônico como uma forma de comunicação jurídica inserida em sistemas digitais. O ponto comum é que o meio tecnológico altera a forma de manifestação da vontade, de documentação e de circulação de informações, mas não elimina exigências de confiança, boa-fé e previsibilidade.

Polido e Silva (2017) acrescentam que a conectividade também amplia a internacionalização das relações privadas. Contratações celebradas em redes digitais podem envolver partes situadas em diferentes jurisdições, infraestruturas distribuídas e prestadores localizados fora do território do consumidor. A consequência é a multiplicação de questões sobre lei aplicável, competência, autenticidade, validade e execução. Para a responsabilidade civil, esse cenário significa que a identificação do responsável não depende apenas de localizar quem praticou materialmente o ato, mas também de definir quais deveres jurídicos incidiam sobre cada agente da cadeia.

Por isso, a adaptação da responsabilidade civil ao ambiente digital exige preservar seus elementos estruturantes, mas reinterpretar o conteúdo dos deveres de diligência. Em relações mediadas por tecnologia, agir de forma diligente pode envolver manter sistemas seguros, informar de maneira compreensível, documentar decisões automatizadas, disponibilizar canais de contestação e controlar riscos previsíveis. A culpa, quando relevante, deixa de ser percebida apenas como desatenção individual e passa a incorporar falhas organizacionais ou técnicas que

poderiam ter sido evitadas por governança adequada.

2.2 Plataformas digitais, conteúdos de terceiros e deveres de cuidado

A responsabilidade das plataformas constitui um dos pontos mais sensíveis da literatura. O problema surge porque esses agentes podem desempenhar papéis distintos: provedores de infraestrutura, redes sociais, mecanismos de busca, marketplaces, ambientes de publicidade, serviços de hospedagem ou intermediários de transações. A intensidade de sua participação interfere diretamente na análise do dever de cuidado. Quanto maior o controle sobre visibilidade, monetização, recomendação, organização da oferta e processamento de dados, menor é a utilidade de uma visão que trate a plataforma como simples espaço neutro.

Brega (2023) discute esse tema a partir da responsabilidade de provedores de redes sociais por conteúdos publicados on-line. O autor mostra que o modelo brasileiro buscou limitar a responsabilidade automática do intermediário e preservar a liberdade de expressão, ao mesmo tempo em que reconheceu deveres relacionados à remoção de conteúdos em determinadas hipóteses. A comparação com a experiência alemã evidencia que transparência, procedimentos e formalização podem ser tão importantes quanto a escolha entre responsabilidade subjetiva ou objetiva.

Tomasevicius Filho (2016), ao analisar o Marco Civil da Internet, já apontava tensões entre a pretensão de regular relações ocorridas em uma rede global e a necessidade de proteger privacidade, honra e imagem. A crítica é relevante porque revela que nenhuma regra de responsabilidade funciona isoladamente: sua efetividade depende de procedimentos capazes de localizar o conteúdo, identificar o agente, preservar provas e permitir respostas proporcionais. Em ambiente de circulação massiva de informações, o tempo de reação pode ser determinante para a extensão do dano.

A discussão ganhou novo significado com o julgamento analisado por Lemos e Estima (2026). Os autores destacam que a controvérsia sobre a responsabilidade das plataformas no Brasil passou a incorporar de maneira mais explícita a agência algorítmica e a forma como sistemas técnicos participam da circulação, recomendação e amplificação de conteúdos. Essa leitura desloca a análise de uma pergunta exclusivamente centrada em “quem publicou” para outra mais ampla: quais agentes contribuíram, por ação ou omissão relevante, para aumentar, manter ou monetizar a exposição ao risco?

Esse deslocamento não implica responsabilidade automática por todo conteúdo ilícito. A própria literatura ressalta a necessidade de critérios de proporcionalidade, previsibilidade e

capacidade de controle. A responsabilidade deve distinguir a autoria do conteúdo, a omissão diante de sinais juridicamente relevantes, a falha de procedimentos, o descumprimento de deveres de segurança e a atuação ativa do sistema de recomendação. Quanto mais específica for a identificação do dever violado, menor o risco de transformar intermediários em censores privados ou seguradores universais de toda atividade realizada por terceiros.

Em marketplaces, a questão assume contornos adicionais porque a plataforma frequentemente organiza pagamentos, reputação, publicidade, busca, ranking e mediação de conflitos. Lemos e Estima (2026) registram que o debate brasileiro recente também alcança a responsabilidade de plataformas que operam mercados digitais. Em perspectiva comparada, a literatura mostra que deveres de informação, identificação do vendedor e tratamento de reclamações podem funcionar como mecanismos relevantes de prevenção. A responsabilidade civil, nesse contexto, conecta-se diretamente à forma concreta de participação do intermediário na relação de consumo.

2.3 Privacidade, proteção de dados e novas formas de dano

A proteção de dados transformou profundamente o debate sobre danos nas relações digitais. Boff e Fortes (2014) situaram a privacidade e a proteção dos dados pessoais no ciberespaço como dimensão fundamental da tutela da pessoa. O ponto é particularmente importante para a responsabilidade civil porque a lesão informacional não se esgota na divulgação pública de um dado íntimo. O dano pode ocorrer pela coleta excessiva, pelo compartilhamento indevido, pela utilização incompatível com a finalidade informada, pela falha de segurança, pela inferência de características sensíveis ou pela formação de perfis capazes de afetar oportunidades e decisões.

Szinvelski, Arceno e Francisco (2019) observam que o big data amplia a capacidade de agregar informações e extrair valor de dados dispersos. Essa dinâmica modifica a escala do problema: elementos aparentemente triviais, quando combinados, podem produzir inferências relevantes sobre hábitos, preferências e comportamentos. Para a responsabilidade civil, isso significa que a avaliação do risco não pode considerar cada dado de maneira isolada; é necessário compreender a capacidade de correlação e o efeito cumulativo do tratamento.

Fornasier e Knebel (2021) aprofundam a crítica ao demonstrar que o consentimento formal do titular ocorre em contexto de intensa assimetria informacional. Nas plataformas digitais, a liberdade de escolha pode ser reduzida por termos extensos, dependência funcional do serviço, desenho de interfaces e falta de alternativas equivalentes. A responsabilidade civil

precisa, portanto, ser articulada com uma ideia material de autonomia. Não basta perguntar se houve um clique de concordância; é necessário verificar se o tratamento observou deveres de informação, finalidade, segurança e respeito às legítimas expectativas do titular.

A elevação da proteção de dados a direito fundamental reforçou essa tendência. Martins (2022) analisa as repercussões da Emenda Constitucional n. 115/2022 e destaca a posição constitucional da proteção de dados no ordenamento brasileiro. Acioly, Silva e Monteiro Neto (2024) examinam o enforcement desse direito e o papel institucional da autoridade de proteção de dados. Embora esses estudos tenham enfoque constitucional e regulatório, suas conclusões afetam diretamente o direito privado: quanto mais clara é a existência de deveres de proteção, mais consistente se torna a análise de ilicitude e de diligência em casos de vazamento, uso incompatível ou tratamento abusivo.

A literatura também evidencia que os danos informacionais podem ser coletivos ou difusos. Silva *et al.* (2022), ao analisarem aplicações de rastreamento de contatos, mostram que tecnologia, finalidade pública e privacidade precisam ser compatibilizadas mediante critérios de proporcionalidade. A conclusão ultrapassa o contexto sanitário: sistemas de alto impacto podem produzir benefícios legítimos e, ainda assim, gerar riscos relevantes se coletarem dados em excesso, não limitarem a finalidade ou mantiverem informações por tempo superior ao necessário. A responsabilidade civil contemporânea, por isso, aproxima-se de uma lógica preventiva, em que a governança do risco antecede o dano consumado.

2.4 Poder econômico, governança e assimetria informacional

As plataformas digitais não são apenas agentes tecnológicos; elas também organizam mercados, estabelecem padrões contratuais e definem condições de acesso a serviços essenciais para a vida social e econômica. Gonçalves, Coutinho e Kira (2022) mostram que a regulação das plataformas envolve desafios de coordenação institucional e de poder econômico. Barros e Prol (2025) avançam nessa direção ao analisar como empresas de tecnologia mobilizam estratégias jurídicas e institucionais para consolidar modelos de negócio e posições de mercado.

Esse contexto é relevante para a responsabilidade civil porque a capacidade de prevenir danos está relacionada ao grau de controle e de informação do agente. Empresas que projetam interfaces, definem parâmetros de recomendação, controlam grandes bases de dados e estabelecem regras privadas de acesso possuem capacidade preventiva superior à do usuário comum. A distribuição dos deveres de cuidado deve refletir essa assimetria. Quando o risco

decorre de escolhas estruturais do modelo de negócio, a análise da diligência não pode ser limitada à conduta do operador final ou do consumidor.

A governança aparece, assim, como ponte entre regulação e responsabilidade civil. Políticas de segurança, mecanismos de auditoria, registros de decisões, avaliações de risco, canais de atendimento e procedimentos de contestação funcionam como evidências da forma pela qual o agente administra riscos previsíveis. Sua ausência não produz automaticamente dever de indenizar, mas pode ser relevante para demonstrar falha de organização, especialmente quando existe relação entre a deficiência de governança e o dano sofrido.

A literatura converge para uma compreensão segundo a qual a responsabilidade civil digital deve observar a posição funcional de cada agente. O usuário que publica um conteúdo ilícito, a plataforma que o recomenda, o anunciante que o financia, o fornecedor que vende produto em marketplace e o controlador que trata dados pessoais ocupam posições distintas. A imputação adequada depende da identificação do dever jurídico específico, da capacidade de controle e da contribuição causal. Essa decomposição evita tanto a impunidade decorrente da dispersão tecnológica quanto a responsabilização excessiva de agentes sem efetivo poder de prevenção.

2.5 Inteligência artificial, decisões automatizadas e causalidade complexa

A inteligência artificial intensifica os problemas já presentes no ambiente digital porque sistemas de aprendizado de máquina podem produzir resultados a partir de relações estatísticas de difícil compreensão para usuários e, em alguns casos, para os próprios operadores. Barroso e Mello (2024) destacam transparência, explicabilidade, segurança, controle humano e responsabilidade como princípios relevantes para a regulação da inteligência artificial. Esses elementos também são centrais para o direito civil, pois interferem na capacidade de demonstrar como uma decisão foi produzida e se o agente adotou medidas razoáveis para prevenir danos.

O nexo causal é um dos pontos mais desafiadores. Em sistemas complexos, o resultado pode depender da base de dados, da arquitetura do modelo, de parâmetros definidos pelo desenvolvedor, de decisões de implantação, de atualizações posteriores e do modo como o usuário interage com a ferramenta. A causalidade não desaparece, mas precisa ser reconstruída em camadas. A pergunta juridicamente relevante não é apenas qual componente “causou” o resultado, mas quais condutas humanas e organizacionais contribuíram de modo relevante para a criação, manutenção ou ampliação do risco.

Santos e Graminho (2024) ilustram esse problema ao examinar a discriminação algorítmica. Decisões automatizadas podem reproduzir padrões discriminatórios existentes nos dados ou criar novas formas de tratamento desigual por meio de variáveis aparentemente neutras. Em tais hipóteses, exigir da vítima conhecimento técnico integral sobre o algoritmo pode tornar a tutela inviável. A discussão jurídica tende, por isso, a valorizar deveres de documentação, explicabilidade, transparência e possibilidade de revisão, que reduzem a assimetria probatória e permitem avaliar a adequação da conduta empresarial.

A responsabilidade relacionada à inteligência artificial também exige diferenciar defeito técnico, uso inadequado, falha de supervisão e decisão empresarial consciente. Uma ferramenta pode funcionar exatamente como foi projetada e, ainda assim, produzir dano porque o contexto de uso não era apropriado ou porque os dados empregados geravam risco previsível. Da mesma forma, um resultado adverso não prova automaticamente defeito. A análise deve considerar finalidade, grau de autonomia, previsibilidade do risco, medidas de teste, supervisão humana e capacidade de intervenção.

Por essa razão, a responsabilidade civil no campo da inteligência artificial tende a assumir função preventiva mais explícita. O foco desloca-se do simples ressarcimento posterior para a criação de incentivos de segurança antes da implantação. Avaliação de impacto, testes, documentação e mecanismos de contestação podem reduzir danos e, ao mesmo tempo, oferecer parâmetros objetivos para a apreciação judicial. O desafio é estabelecer deveres proporcionais ao risco, evitando tanto a negligência tecnológica quanto exigências incompatíveis com a natureza experimental da inovação.

3. METODOLOGIA

Foi realizada uma revisão narrativa estruturada da literatura jurídica e interdisciplinar, com recorte temático centrado em responsabilidade civil, plataformas digitais, proteção de dados, contratos eletrônicos, inteligência artificial e regulação de riscos tecnológicos. A base escolhida foi a SciELO, por disponibilizar artigos científicos com metadados verificáveis, indicação de periódico, autoria, ano, volume, páginas ou identificador eletrônico e, na maior parte dos casos, DOI. A busca e a conferência bibliográfica foram realizadas em setembro de 2026.

Foram empregados descritores em português e combinações equivalentes, entre os quais “responsabilidade civil”, “plataformas digitais”, “internet”, “proteção de dados”, “privacidade”, “big data”, “contrato eletrônico”, “comércio eletrônico”, “inteligência artificial” e

“discriminação algorítmica”. Foram incluídos artigos publicados entre 2000 e 2026 que abordassem diretamente problemas jurídicos ou regulatórios ligados às relações digitais e contribuíssem para a análise de pelo menos um dos seguintes eixos: imputação de danos, dever de cuidado, proteção de dados, contratação eletrônica, regulação de plataformas ou decisão algorítmica.

Foram excluídos livros, capítulos, trabalhos de conclusão, relatórios sem avaliação editorial, notícias, páginas institucionais e textos cujo conteúdo não apresentasse relação direta com o problema investigado. O corpus final reuniu dezesseis artigos científicos indexados, utilizados tanto na fundamentação quanto na elaboração das sínteses analíticas. Não se atribuiu ao procedimento caráter de revisão sistemática exaustiva, pois o objetivo foi construir uma análise jurídico-conceitual consistente e verificável, sem estimar prevalências ou produzir meta-análise.

A análise foi qualitativa e temática. Os estudos foram lidos a partir de seis categorias: transformação da contratação e da confiança no ambiente digital; responsabilidade de intermediários e plataformas; privacidade e proteção de dados; poder econômico e governança de plataformas; automação e discriminação algorítmica; e atualização dos critérios de imputação. A comparação entre os artigos permitiu identificar convergências, tensões e lacunas, especialmente quanto à extensão dos deveres preventivos, à prova do nexo causal em sistemas complexos e à relação entre inovação tecnológica e proteção da pessoa.

4. DESENVOLVIMENTO

4.1 Síntese dos estudos selecionados

O Quadro 1 sintetiza o corpus principal da revisão. A seleção foi organizada por eixo temático e evidencia a progressiva passagem de problemas inicialmente concentrados em contratos eletrônicos e privacidade para questões de governança de plataformas, proteção de dados, poder econômico e inteligência artificial. Todos os trabalhos listados foram conferidos em registro indexado na SciELO e utilizados na construção da análise.

Quadro 1. Síntese dos principais artigos indexados utilizados na revisão

Referência	Eixo	Contribuição central
Forgioni (2000)	Contratos e e-commerce	Formação, prova e equilíbrio entre segurança do comércio e proteção do consumidor.
Barreto (2009)	Contrato eletrônico	Contrato digital como estrutura híbrida e necessidade de adaptação da dogmática contratual.
Boff; Fortes (2014)	Privacidade e dados	Reconhecimento da privacidade e dos dados pessoais como dimensão fundamental no

		ciberespaço.
Tomasevicius Filho (2016)	Marco Civil da Internet	Limites e insuficiências regulatórias diante de privacidade, honra e imagem.
Polido; Silva (2017)	Contratos transnacionais	Problemas de lei aplicável, validade e segurança jurídica em contratos eletrônicos internacionais.
Szinvelski; Arceno; Francisco (2019)	Big data	Riscos do tratamento massivo e necessidade de proteção jurídica dos dados pessoais.
Fornasier; Knebel (2021)	Capitalismo de vigilância	Assimetria informacional, monetização de dados e limites do consentimento.
Gonçalves; Coutinho; Kira (2022)	Regulação de plataformas	Poder econômico, coordenação institucional e desafios regulatórios das plataformas digitais.
Martins (2022)	Proteção de dados	Reforço constitucional da proteção de dados e repercussões sobre competências e tutela jurídica.
Silva <i>et al.</i> (2022)	Privacidade e proporcionalidade	Critérios de proporcionalidade aplicados a tecnologias de tratamento de dados em larga escala.
Brega (2023)	Conteúdo em redes sociais	Responsabilidade de provedores e equilíbrio entre remoção, transparência e liberdade de expressão.
Barroso; Mello (2024)	Inteligência artificial	Transparência, explicabilidade, segurança, controle humano e responsabilidade.
Santos; Graminho (2024)	Discriminação algorítmica	Limites jurídicos para decisões automatizadas e proteção contra tratamento discriminatório.
Acioly; Silva; Monteiro Neto (2024)	Enforcement de dados	Instituições, fiscalização e efetividade da proteção de dados pessoais.
Barros; Prol (2025)	Poder das plataformas	Estratégias empresariais, concentração econômica e uso do direito por plataformas digitais.
Lemos; Estima (2026)	Responsabilidade de plataformas	Releitura da responsabilidade civil a partir da materialidade e da agência algorítmica das plataformas.

Fonte: elaborado pelos autores com base em artigos indexados na SciELO (2000–2026).

A síntese evidencia três movimentos. O primeiro é a continuidade: problemas tradicionais de formação contratual, boa-fé, privacidade e dano permanecem presentes. O segundo é a complexificação: plataformas, big data e algoritmos aumentam a distância entre a vítima e os processos que geram o resultado danoso. O terceiro é a prevenção: cresce a importância de deveres organizacionais e procedimentais, como segurança, transparência, documentação, mecanismos de reclamação e revisão. Esses movimentos sugerem que a evolução da responsabilidade civil é incremental e funcional, e não uma ruptura completa com o modelo tradicional.

4.2 Desafios jurídicos para a responsabilidade civil contemporânea

O primeiro desafio é a identificação do agente responsável em cadeias digitais complexas. Um serviço pode envolver desenvolvedor, operador, provedor de nuvem, plataforma, anunciante, fornecedor e usuário. A simples presença de múltiplos atores não autoriza solidariedade automática, mas exige mapear deveres e contribuições. A imputação deve ser funcional: responde quem violou dever próprio e cuja conduta apresenta relação juridicamente relevante com o dano. Essa lógica impede que a fragmentação técnica se converta em vazio de responsabilidade.

O segundo desafio é o nexo causal. Em ambientes algorítmicos, decisões são produzidas por cadeias de processamento que podem ser opacas. A vítima raramente possui acesso a logs, modelos ou critérios de recomendação. Por isso, regras probatórias e deveres de documentação tornam-se centrais. Transparência não é apenas valor regulatório; ela pode ser condição prática para a própria aplicação da responsabilidade civil. Sem acesso mínimo à trajetória decisória, a exigência de prova pode transformar-se em barreira insuperável.

O terceiro desafio é definir o conteúdo do dever de cuidado. A diligência digital precisa ser proporcional ao risco e à capacidade do agente. Para uma plataforma de grande escala, podem ser razoáveis controles, canais de denúncia, políticas de segurança e sistemas de auditoria que seriam desproporcionais para um pequeno prestador. A boa prática regulatória, portanto, deve evitar soluções uniformes e considerar escala, natureza do serviço, vulnerabilidade dos usuários e gravidade potencial do dano.

O quarto desafio é reconhecer danos que não se apresentam imediatamente como perda econômica. Vazamentos, perfilamento, exposição de dados, perda de controle sobre informações e decisões discriminatórias atingem autonomia e personalidade. A literatura sobre proteção de dados mostra que a tutela civil precisa dialogar com a dimensão existencial do dano, sem banalizá-la. Nem toda irregularidade administrativa produz indenização, mas violações relevantes de direitos da personalidade não podem ser reduzidas à ausência de prejuízo patrimonial mensurável.

O quinto desafio é compatibilizar prevenção e inovação. Uma responsabilidade excessivamente ampla pode incentivar bloqueios, remoções preventivas, concentração de mercado e redução de experimentação tecnológica. Por outro lado, a ausência de deveres claros transfere o custo dos riscos para usuários e vítimas. O equilíbrio depende de critérios graduais de responsabilidade, capazes de considerar previsibilidade, controle, benefício econômico, possibilidade de prevenção e resposta posterior ao incidente.

O sexto desafio é a transnacionalidade. Plataformas e serviços operam por infraestruturas distribuídas, enquanto os sistemas de responsabilidade civil permanecem ancorados em jurisdições nacionais. Polido e Silva (2017) demonstram que contratos eletrônicos internacionais já revelavam essa tensão. Em plataformas contemporâneas, ela é ampliada por fluxos globais de dados e decisões automatizadas. Cooperação regulatória, representação local e mecanismos eficazes de execução tornam-se elementos necessários para que a tutela civil não seja apenas formal.

Por fim, a responsabilidade civil digital deve ser compreendida como parte de uma arquitetura mais ampla de governança. Indenização posterior é importante, mas não substitui prevenção, fiscalização, normas de proteção de dados, defesa do consumidor e mecanismos internos de correção. O modelo mais consistente é aquele que usa a responsabilidade civil para alinhar incentivos: quem possui maior capacidade de prevenir determinado risco deve ser estimulado a fazê-lo, sem que isso elimine a responsabilidade primária de quem pratica diretamente o ilícito.

5. CONSIDERAÇÕES FINAIS

A revisão demonstra que a responsabilidade civil continua sendo instrumento indispensável de tutela nas relações digitais, mas sua aplicação exige uma leitura atualizada das categorias tradicionais. Conduta, dano e nexo causal permanecem fundamentais, porém são examinados em ambientes marcados por intermediação, automação, tratamento massivo de dados e distribuição de decisões entre múltiplos agentes. A principal mudança não está na criação de uma responsabilidade totalmente nova, mas na transformação do conteúdo dos deveres de diligência.

Nos contratos eletrônicos, a atenção desloca-se para informação, prova, segurança e confiança. Nas plataformas, a discussão envolve grau de intervenção, capacidade de controle, recomendação algorítmica e procedimentos de resposta. Na proteção de dados, ganha relevo a prevenção de danos informacionais e a proteção da autonomia do titular. Na inteligência artificial, a análise depende de documentação, explicabilidade, supervisão e reconstrução da cadeia causal. Esses campos convergem na exigência de governança proporcional ao risco.

A literatura também afasta duas soluções simplificadoras. De um lado, não é adequado tratar toda plataforma ou tecnologia como responsável automática por qualquer dano relacionado ao serviço. De outro, a ideia de neutralidade técnica não pode ser utilizada para ocultar decisões empresariais que influenciam exposição, recomendação, monetização ou

tratamento de informações. A atribuição de responsabilidade deve observar a função concreta do agente e o dever jurídico que estava em condições de cumprir.

Em termos probatórios, um dos desafios mais relevantes é a assimetria entre vítima e fornecedor de tecnologia. Informações necessárias à reconstrução do fato frequentemente permanecem sob controle do próprio agente econômico. Por isso, deveres de registro, transparência e cooperação processual possuem importância crescente. Tais mecanismos não antecipam culpa, mas tornam possível verificar se houve diligência suficiente e se determinada escolha técnica contribuiu para o dano.

A proteção de dados evidencia, ainda, que a noção de dano precisa considerar dimensões existenciais e informacionais. A exposição indevida, o uso incompatível de dados e o perfilamento discriminatório podem atingir direitos da personalidade mesmo quando não há perda patrimonial imediata. A resposta jurídica deve evitar indenizações automáticas por qualquer irregularidade, mas precisa reconhecer situações em que a violação produz impacto relevante sobre autonomia, privacidade, reputação ou acesso a oportunidades.

No campo da inteligência artificial, o principal desafio é impedir que a complexidade técnica produza irresponsabilidade difusa. Sistemas automatizados são desenvolvidos, treinados, configurados, implementados e supervisionados por pessoas e organizações. A autonomia tecnológica modifica a cadeia causal, mas não elimina a necessidade de atribuir deveres a quem seleciona o contexto de uso, define parâmetros, disponibiliza o sistema ou se beneficia economicamente da operação. A responsabilidade deve ser calibrada conforme previsibilidade, controle e possibilidade de prevenção.

Como limitação, esta pesquisa adotou revisão narrativa estruturada e corpus concentrado em artigos indexados na SciELO, não pretendendo representar toda a literatura nacional e internacional sobre responsabilidade civil digital. Essa escolha, contudo, permitiu trabalhar exclusivamente com referências verificáveis em base científica e construir uma síntese coerente do debate brasileiro contemporâneo. Estudos futuros podem ampliar o corpus para outras bases, comparar regimes estrangeiros de responsabilidade por inteligência artificial e investigar decisões judiciais a partir de métodos empíricos.

Conclui-se que a responsabilidade civil na sociedade digital deve combinar reparação e prevenção. A tutela efetiva não depende apenas de indenizar depois do dano, mas de criar incentivos para que plataformas, controladores de dados, fornecedores e desenvolvedores adotem medidas compatíveis com os riscos que controlam. Transparência, segurança, documentação, canais de contestação e supervisão humana não substituem os fundamentos do

direito privado; ao contrário, atualizam o significado da diligência em um ambiente tecnológico. O desafio contemporâneo é preservar a inovação e a liberdade de circulação sem transformar a complexidade digital em obstáculo à proteção da pessoa.

5. CONFLITO DE INTERESSES

Os autores declaram que não há conflito de interesses de natureza pessoal, financeira, profissional ou institucional que possa ter influenciado a elaboração, a análise ou a interpretação deste trabalho.

6. REFERÊNCIAS

ACIOLY, Luis Henrique de Menezes; SILVA, Matheus Fernandes da; MONTEIRO NETO, João Araújo. A Emenda Constitucional nº 115 de 10 de fevereiro de 2022 e o enforcement da proteção de dados pessoais no Brasil. **Revista de Investigações Constitucionais**, Curitiba, v. 11, n. 3, e275, 2024. DOI: <https://doi.org/10.5380/rinc.v11i3.92117>.

BARRETO, Ricardo Menna. Contrato eletrônico como cibercomunicação jurídica. **Revista Direito GV**, São Paulo, v. 5, n. 2, p. 443-458, 2009. DOI: <https://doi.org/10.1590/S1808-24322009000200010>.

BARROS, Caetano Patta da Porciuncula e; PROL, Flávio Marques. Direito e economia política nas estratégias empresariais de plataformas digitais no Brasil: apontamentos para uma agenda de pesquisa. **Revista Direito e Práxis**, Rio de Janeiro, v. 16, n. 2, e89210, 2025. DOI: <https://doi.org/10.1590/2179-8966/2025/89210>.

BARROSO, Luís Roberto; MELLO, Patrícia Perrone Campos. Inteligência artificial: promessas, riscos e regulação. Algo de novo debaixo do sol. **Revista Direito e Práxis**, Rio de Janeiro, v. 15, n. 4, e84479, 2024. DOI: <https://doi.org/10.1590/2179-8966/2024/84479>.

BOFF, Salete Oro; FORTES, Vinícius Borges. A privacidade e a proteção dos dados pessoais no ciberespaço como um direito fundamental: perspectivas de construção de um marco regulatório para o Brasil. **Sequência: Estudos Jurídicos e Políticos**, Florianópolis, v. 35, n. 68, p. 109-127, 2014. DOI: <https://doi.org/10.5007/2177-7055.2013v35n68p109>.

BREGA, Gabriel Ribeiro. A regulação de conteúdo nas redes sociais: uma breve análise comparativa entre o NetzDG e a solução brasileira. **Revista Direito GV**, São Paulo, v. 19, e2305, 2023. DOI: <https://doi.org/10.1590/2317-6172202305>.

FORGIONI, Paula A. Apontamentos sobre aspectos jurídicos do e-commerce. **Revista de Administração de Empresas**, São Paulo, v. 40, n. 4, p. 70-83, 2000. DOI: <https://doi.org/10.1590/S0034-75902000000400007>.

FORNASIER, Mateus de Oliveira; KNEBEL, Norberto Milton Paiva. O titular de dados como sujeito de direito no capitalismo de vigilância e mercantilização dos dados na Lei Geral de Proteção de Dados. **Revista Direito e Práxis**, Rio de Janeiro, v. 12, n. 2, p. 1002-1033, 2021. DOI: <https://doi.org/10.1590/2179-8966/2020/46944>.

GONÇALVES, Priscila Brolio; COUTINHO, Diogo R.; KIRA, Beatriz. Vírus e Telas: o direito econômico das plataformas digitais na pandemia de COVID-19. **Revista Direito e Práxis**, Rio de Janeiro, v. 13, n. 1, p. 44-68, 2022. DOI: <https://doi.org/10.1590/2179-8966/2020/51741>.

LEMO, André; ESTIMA, Waldir. Responsabilidade civil das plataformas digitais no Brasil: a materialidade das plataformas na análise do julgamento do STF. **Galáxia**, São Paulo, v. 51, e73593, 2026. DOI: <https://doi.org/10.1590/1982-2553202673593>.

MARTINS, Ricardo Marcondes. Proteção de dados, competências dos entes federativos e a Emenda Constitucional n. 115/22. **Revista de Investigações Constitucionais**, Curitiba, v. 9, n. 3, p. 645-658, 2022. DOI: <https://doi.org/10.5380/rinc.v9i3.87107>.

POLIDO, Fabrício Bertini Pasquot; SILVA, Lucas Sávio Oliveira da. Contratos internacionais eletrônicos e o direito brasileiro: entre a insuficiência normativa doméstica e as soluções globais. **Sequência: Estudos Jurídicos e Políticos**, Florianópolis, v. 38, n. 75, p. 157-188, 2017. DOI: <https://doi.org/10.5007/2177-7055.2017v38n75p157>.

SANTOS, Rodrigo Coimbra; GRAMINHO, Vivian Maria Caxambu. Discriminação algorítmica nas relações de trabalho e princípios da Lei Geral de Proteção de Dados. **Sequência: Estudos Jurídicos e Políticos**, Florianópolis, v. 45, n. 96, e96294, 2024. DOI: <https://doi.org/10.5007/2177-7055.2024.e96294>.

SILVA, Ana Marília Dutra Ferreira da *et al.* Proteção de dados pessoais e direito à privacidade no contexto da pandemia de COVID-19: uma análise das aplicações de contact tracing à luz da proporcionalidade. **Revista Direito GV**, São Paulo, v. 18, n. 3, e2232, 2022. DOI: <https://doi.org/10.1590/2317-6172202232>.

SZINVELSKI, Martín Marks; ARCENO, Taynara Silva; FRANCISCO, Lucas Baratieri. Perspectivas jurídicas da relação entre big data e proteção de dados. **Perspectivas em Ciência da Informação**, Belo Horizonte, v. 24, n. 4, p. 132-144, 2019. DOI: <https://doi.org/10.1590/1981-5344/4188>.

TOMASEVICIUS FILHO, Eduardo. Marco Civil da Internet: uma lei sem conteúdo normativo. **Estudos Avançados**, São Paulo, v. 30, n. 86, p. 269-285, 2016. DOI: <https://doi.org/10.1590/S0103-40142016.00100017>.