PONTIFÍCIA UNIVERSIDADE CATÓLICA DE SÃO PAULO – PUC/SP

FACULDADE DE DIREITO

Aluno: André Carneiro Gomez

RA00305306

RESPONSABILIDADE CIVIL E INTELIGÊNCIA ARTIFICIAL: *CHATBOTS* E A RESPONSABILIDADE NO FORNECIMENTO DE INFORMAÇÕES EQUÍVOCAS E FRAUDULENTAS PELAS EMPRESAS DE TECNOLOGIA

Projeto de Trabalho de Conclusão de Curso

Orientadora: Déborah Regina Lambach Ferreira da Costa

São Paulo

2025

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE SÃO PAULO – PUC/SP

FACULDADE DE DIREITO

DEPARTAMENTO DE DIREITO CIVIL, PROCESSUAL CIVIL E DO TRABALHO

Trabalho de Conclusão de Curso apresentado à banca examinadora da Pontifícia Universidade Católica de São Paulo, como exigência parcial para obtenção do título de BACHAREL em Direito, sob orientação da Professora Doutora Déborah Regina Lambach Ferreira da Costa.

São Paulo

2025

Banca Examinadora

_____

_____

_____

_____

_____

À comunidade da Pontifícia Universidade Católica de São Paulo pelo apoio permanente.

AGRADECIMENTOS

Agradeço, de maneira especial, à minha orientadora, Professora Doutora Déborah Regina Lambach Ferreira da Costa, pela orientação criteriosa, pela disponibilidade constante e pelo valioso suporte intelectual prestado durante todas as etapas desta pesquisa. Sua condução segura e generosa foi fundamental para o amadurecimento deste trabalho e para minha formação acadêmica.

Estendo meus sinceros agradecimentos a todos os professores que integraram minha trajetória na Pontifícia Universidade Católica de São Paulo. Cada ensinamento transmitido, cada reflexão provocada e cada contribuição metodológica foram indispensáveis para a consolidação dos conhecimentos que sustentam esta monografia.

Aos meus pais, Patricia e Sergio, registro minha mais profunda e respeitosa gratidão. O apoio incondicional, os valores éticos e a dedicação com que sempre nortearam minha educação foram determinantes para que eu alcançasse este marco em minha vida acadêmica. Esta conquista é, em grande parte, reflexo do esforço e da confiança que sempre depositaram em mim.

Aos meus amigos, Bruno Justo, Ilan Hirata, João Pedro Guerra, João Pedro Paixão, Laís de Carvalho, Mariana Noronha, Sofia Cheib, Stephanie Cunha, Vera Gomes, e Vinicius Martinez, cuja presença firme se fez sentir nos momentos de desafio e superação, deixo meu reconhecimento e apreço. As palavras de incentivo, o companheirismo e a compreensão foram essenciais para que eu pudesse perseverar com serenidade e equilíbrio ao longo da jornada universitária.

A Excelentissima Senhora Doutora Juíza Gabriela Fragoso Calasso Costa, na qual tive a honra de estagiar em seu gabinete, durante dois anos. Agradeço por toda a confiança e aprendizado, que ajudou a me tornar, não só como um profissional e acadêmico do Direito competente, mas como uma pessoa melhor.

A todas as pessoas que, direta ou indiretamente, contribuíram para a realização deste trabalho, manifesto meus mais sinceros agradecimentos.

A educação é a arma mais poderosa que você pode usar para mudar o mundo. (MANDELA, 2003).

RESUMO

GOMEZ, André Carneiro. **Responsabilidade Civil e Inteligência Artificial**: *Chatbots* e a responsabilidade no Fornecimento de informações equívocas e fraudulentas pelas empresas de tecnologia.

Este trabalho analisa, sob uma perspectiva crítica e jurídico-sistemática, a responsabilidade civil das empresas de tecnologia pelo fornecimento de informações equívocas ou fraudulentas por meio de *chatbots* operados por inteligência artificial (IA). Parte-se do problema de que o atual ordenamento jurídico brasileiro não oferece respostas suficientemente eficazes diante das novas relações entre usuários e agentes artificiais. A hipótese central sustenta que os sistemas normativos existentes apresentam lacunas e inadequações frente aos danos ocasionados por sistemas automatizados de conversação. O objetivo geral consiste em examinar as bases legais da responsabilização civil — objetiva e subjetiva — à luz da Constituição Federal, do Código Civil, da Lei Geral de Proteção de Dados (LGPD) e do Código de Defesa do Consumidor (CDC), articulando tais normas com os riscos e impactos do uso de *machine learning* na sociedade digital. A pesquisa se desenvolve por meio de análise bibliográfica e documental, com enfoque qualitativo e abordagem hipotético-dedutiva, apoiada em doutrina, jurisprudência e normas legais nacionais e estrangeiras. Os objetivos específicos envolvem: o estudo evolutivo e conceitual da IA; a delimitação dos deveres informacionais das empresas de tecnologia; o mapeamento dos riscos jurídicos oriundos de erros ou manipulações algorítmicas; a avaliação das insuficiências regulatórias atuais; e a formulação de propostas para um marco normativo eficaz. Os resultados obtidos apontam para a necessidade urgente de regulamentações específicas que considerem a assimetria informacional entre usuários e empresas, bem como o potencial lesivo dos algoritmos autônomos. Defende-se a construção de um modelo jurídico propositivo, que contemple tanto instrumentos estatais quanto mecanismos de autorregulação tecnológica, com vistas à tutela dos direitos fundamentais e à promoção de maior segurança jurídica nas relações digitais. Conclui-se que o desafio contemporâneo da responsabilidade civil na era da IA exige uma renovação paradigmática dos fundamentos jurídicos tradicionais.

Palavras-chave: Responsabilidade civil; Inteligência artificial; *Chatbots*; Desinformação algorítmica; Marco regulatório.

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
CC	Código Civil de 2002
CDC	Código de Defesa do Consumidor
CRFB	Constituição da República Federativa do Brasil de 1988
CPC	Código de Processo Civil de 2015
EBIA	Estratégia Brasileira de Inteligência Artificial
IA	Inteligência Artificial
LGPD	Lei Geral de Proteção de Dados
NBR	Normas Técnicas Brasileiras
OCDE	Organização para a Cooperação e Desenvolvimento Econômico
PL	Projeto de Lei
PLN	Processamento de Linguagem Natural
TCC	Trabalho de Conclusão de Curso
UE	União Européia

SUMÁRIO

INTRODUÇÃO

O avanço da inteligência artificial (IA) e sua aplicação crescente nos processos empresariais vêm transformando profundamente as formas de interação entre consumidores e prestadores de serviços. Entre essas aplicações, destacam-se os *chatbots* — programas baseados em algoritmos de linguagem natural e aprendizado de máquina — como ferramentas cada vez mais utilizadas no atendimento ao cliente, na divulgação de informações e na realização de transações comerciais. Apesar de seus benefícios operacionais e econômicos, esses sistemas apresentam riscos significativos, especialmente quando fornecem respostas incorretas, enganosas ou fraudulentas, com potencial de causar prejuízos materiais e danos morais aos usuários.

O presente trabalho tem como objetivo examinar, sob a perspectiva do ordenamento jurídico brasileiro, os parâmetros legais da responsabilidade civil aplicável às empresas de tecnologia que desenvolvem ou operam sistemas de IA, com foco específico nos *chatbots*. Parte-se do entendimento de que os danos provocados por essas ferramentas não devem ser compreendidos como meros erros técnicos, mas como eventos juridicamente relevantes, cuja gravidade exige a análise de mecanismos legais de reparação fundamentados no Código Civil, na Constituição Federal e na Lei Geral de Proteção de Dados (LGPD).

Inicialmente, são apresentados os principais conceitos e a evolução histórica da inteligência artificial, destacando seu impacto em diferentes setores e os fundamentos técnicos por trás do funcionamento dos *chatbots*. Na sequência, aborda-se a estrutura da responsabilidade civil no direito brasileiro, com ênfase na distinção entre responsabilidade objetiva e subjetiva e sua adaptação às demandas da era digital. Também são analisados o papel da função social da responsabilidade e a importância da boa-fé nas relações jurídicas mediadas por tecnologia.

Além disso, explora-se o dever de informar das empresas que operam sistemas de IA, considerando os requisitos legais de veracidade, transparência e atualização das informações fornecidas. A análise inclui ainda os desafios associados à transparência algorítmica e à responsabilização dos fornecedores frente aos conteúdos gerados por sistemas automatizados.

No campo da proteção de dados, examina-se a LGPD em seus aspectos constitucionais e infraconstitucionais, destacando os direitos dos titulares de dados pessoais, o consentimento informado e as obrigações relacionadas à segurança da informação. O objetivo é compreender como essa legislação se aplica aos sistemas de IA e como pode contribuir para a responsabilização das empresas quando ocorrem falhas informacionais que afetam os usuários.

Em continuidade, são discutidas as implicações jurídicas do fornecimento de dados ou informações incorretas por inteligências artificiais, incluindo os danos patrimoniais e extrapatrimoniais que podem ser causados aos usuários. A análise é enriquecida com decisões judiciais nacionais e internacionais, que refletem os caminhos trilhados pelo Judiciário no enfrentamento dessa temática complexa e atual.

Por fim, analisam-se os desafios regulatórios associados à inteligência artificial, propondo uma reflexão sobre os limites da legislação vigente e apontando caminhos para o desenvolvimento de uma regulação mais eficaz. São consideradas propostas legislativas em trâmite, princípios éticos e modelos de governança algorítmica que buscam equilibrar inovação tecnológica, segurança jurídica e proteção de direitos fundamentais.

Ao final, pretende-se oferecer uma contribuição crítica e propositiva para a construção de um arcabouço normativo que assegure a responsabilização justa das empresas de tecnologia e a proteção eficaz dos usuários em um ambiente digital marcado pela crescente automação e pela complexidade das interações mediadas por inteligências artificiais.

1 INTELIGÊNCIA ARTIFICIAL E O USO DE *CHATBOTS* NO CONTEXTO DIGITAL

A ascensão da Inteligência Artificial representa um dos mais significativos vetores de transformação no cenário tecnológico contemporâneo, redefinindo paradigmas em múltiplos domínios da atividade humana.

Neste contexto de inovação acelerada, os chatbots surgiram como uma das manifestações mais proeminentes e difundidas da IA remodelando as dinâmicas de interação no ambiente digital. A transição de sistemas simples, baseados em regras predefinidas, para plataformas sofisticadas que empregam Processamento de Linguagem Natural (PLN) e machine learning, marcou uma evolução crítica, permitindo que essas tecnologias não apenas compreendam, mas também interpretem a intenção, o contexto e as necessidades humanas.

A crescente integração de chatbots em setores evidenciam uma mudança substancial na forma como as organizações se comunicam com seus públicos e como os indivíduos acessam informação e serviços. Essa onipresença suscita uma análise aprofundada tanto das oportunidades, quanto dos desafios inerentes a essa tecnologia.

Por um lado, os chatbots oferecem uma comunicação mais eficiente, personalizada e disponível ininterruptamente. Por outro, levantam questões críticas relativas à privacidade de dados, à automação do trabalho, à confiabilidade da informação e aos potenciais vícios de algorítmicos.

Este capítulo se propõe a explorar a complexa intersecção entre a Inteligência Artificial e a aplicação de chatbots no ecossistema digital. Ao longo dos subcapítulos subsequentes, será realizada uma análise de conceitos básicos, a evolução histórica desses sistemas, as diversas aplicações em diversos setores e o funcionamento da IA.

1.1 Conceito e evolução da inteligência artificial

O rápido avanço da tecnologia digital e a sofisticação crescente dos sistemas baseados em inteligência artificial (IA) têm resultado na ampla utilização de *chatbots* como instrumentos essenciais nas interações sociais, comerciais e institucionais contemporâneas. Tais sistemas automatizados vêm sendo progressivamente adotados por diversas organizações devido à sua capacidade para aprimorar o

atendimento ao consumidor, aumentando a eficiência operacional e gerando redução expressiva de custos. Contudo, apesar dos reconhecidos benefícios que essas tecnologias proporcionam, emergem uma complexa e desafiante gama de riscos jurídicos, especialmente relacionada à produção e disseminação de informações incorretas, enviesadas ou fraudulentas.

Nesse contexto, Shoshana Zuboff (2019) fornece uma contribuição relevante ao propor uma análise crítica acerca do capitalismo de vigilância, paradigma econômico predominante na atualidade, que transforma experiências humanas em recursos exploráveis para fins mercadológicos, predições e intervenções comportamentais. Zuboff argumenta que essa nova lógica econômica é parasitária, fundamentando-se em práticas invasivas de coleta de dados em larga escala, nas quais o comportamento humano é expropriado continuamente para alimentar mecanismos avançados de previsão e manipulação comercial. Tal abordagem não apenas compromete a privacidade, mas subverte também a própria autonomia individual, transformando seres humanos em meras fontes de superávit comportamental.

Essa dinâmica de exploração, segundo a autora, gera novos e alarmantes desafios éticos e jurídicos, ao se considerar que os dados obtidos são utilizados não apenas para prever comportamentos, mas também para moldá-los. Consequentemente, essa mesma lógica operacional é identificável na utilização de *chatbots*, cujos sistemas automatizados podem amplificar os riscos de danos materiais e extrapatrimoniais por meio de erros sistemáticos ou fraudes informacionais no ambiente digital.

Yuval Noah Harari (2024) corrobora essa perspectiva ao enfatizar que a intensificação da dependência de tecnologias baseadas em inteligência artificial ampliou a frequência e a escala dos erros, contribuindo para a disseminação de informações imprecisas, enviesadas ou mesmo inteiramente falsas.

De acordo com Harari, sistemas algorítmicos, embora dotados de impressionante capacidade analítica, refletem preconceitos e distorções embutidos nos próprios dados que os alimentam.

Além disso, o autor destaca que tais tecnologias podem agravar conflitos sociais e manipular decisões individuais e coletivas, criando uma falsa percepção de neutralidade e objetividade.

Esses equívocos algorítmicos possuem um elevado potencial destrutivo, podendo ocasionar não apenas prejuízos financeiros substanciais, mas também comprometer a integridade moral dos indivíduos e violar gravemente direitos fundamentais coletivos e individuais, questionando inclusive a própria base democrática das sociedades contemporâneas.

Do ponto de vista jurídico, a responsabilidade civil pelos danos decorrentes do uso de *chatbots* permanece permeada por dúvidas conceituais e dificuldades práticas. Embora o Código Civil brasileiro estabeleça, em determinadas circunstâncias, a responsabilidade civil objetiva, inexiste uma regulamentação específica quanto aos danos oriundos de agentes autônomos artificiais, como é o caso dos *chatbots* (Código Civil de 2002).

Da mesma forma, apesar da Lei Geral de Proteção de Dados (LGPD) estabelecer uma estrutura normativa sólida voltada à proteção de dados pessoais, essa legislação apresenta limitações evidentes quando se trata de se regular situações envolvendo erros ou fraudes praticados por sistemas dotados de inteligência artificial, especialmente no ambiente interativo dos *chatbots* (LGPD).

Frente a esse cenário marcado por incertezas normativas e lacunas jurídicas, torna-se imprescindível aprofundar estudos acerca da responsabilidade civil das empresas que desenvolvem e utilizam tais tecnologias, particularmente nos casos em que *chatbots* causam prejuízos diretos ou indiretos mediante informações falsas ou fraudulentas. Torna-se essencial investigar de maneira teórica e empírica como esses novos desafios podem ser enfrentados e solucionados pelo sistema jurídico vigente.

Além disso, faz-se necessário abordar os princípios éticos e regulatórios relacionados à utilização de IA, refletindo sobre como tais diretrizes podem contribuir para o desenvolvimento de uma estrutura normativa mais abrangente e efetiva. Essa estrutura deverá garantir tanto a proteção dos usuários quanto a responsabilização

das empresas tecnológicas por práticas inadequadas ou ilícitas realizadas por seus sistemas automatizados.

1.2 Aplicações práticas dos *chatbots* em diferentes setores

Na era da transformação digital, os *chatbots* representam uma das tecnologias mais disruptivas e eficazes para revolucionar o atendimento ao cliente e otimizar processos organizacionais em praticamente todos os setores da economia. Essas ferramentas, baseadas em inteligência artificial, simulam conversas humanas por meio de interfaces conversacionais interativas, destacando-se como soluções estratégicas essenciais para empresas que buscam competitividade, eficiência operacional e excelência no relacionamento com seus clientes.

No contexto brasileiro, a adoção de *chatbots* também se mostra expressiva e em ascensão. O Brasil já figura entre os cinco países que mais utilizam *chatbots*, ao lado de Estados Unidos, Índia, Alemanha e Reino Unido.

Essa posição de destaque reflete tanto o esforço de digitalização de organizações públicas e privadas quanto a receptividade dos usuários brasileiros a interações automatizadas. Um estudo de 2023 apontou que aproximadamente 47% dos Centros de Serviços Compartilhados (CSC) no Brasil já empregam *chatbots* em seus fluxos de trabalho, especialmente em departamentos de Recursos Humanos e TI, visando maximizar eficiência e produtividade (IEG, 2024).

Além disso, o governo brasileiro lançou estratégias nacionais de Transformação Digital e IA, prevendo investimentos significativos (da ordem de dezenas de bilhões de reais) para fomentar tecnologias voltadas à melhora de serviços públicos e processos internos. No setor privado, uma pesquisa da consultoria Gartner destacada em 2022 revelou que metade dos líderes empresariais já enxergava valor no uso de *chatbots* e estimou-se que 40% das empresas adotariam *chatbots* em suas operações até 2024 (CAMPOS, 2024).

1.2.1 *Chatbots* no Setor Jurídico

O setor jurídico tradicionalmente lida com grandes volumes de informações, linguagem altamente especializada e demandas por celeridade. Nesse contexto, os *chatbots* e outras soluções de IA vêm sendo incorporados para aumentar a eficiência de escritórios de advocacia, departamentos jurídicos corporativos e até mesmo órgãos do Judiciário. Em escritórios de advocacia, por exemplo, *chatbots* baseados em PLN podem atuar como assistentes virtuais no atendimento a clientes, esclarecendo dúvidas iniciais, agendando consultas e fazendo triagens de casos de forma ágil.

Uma pesquisa da Gartner indicou que, já em 2022, 50% dos líderes jurídicos que adotaram essas ferramentas relataram ganhos de produtividade, e esperava-se que a adoção se ampliasse significativamente em 2023 e 2024 (CAMPOS, 2024). Esses *chatbots jurídicos* geralmente são integrados a sites ou aplicativos de mensagem (como WhatsApp), permitindo que clientes consultem o andamento de seus processos ou obtenham respostas para perguntas frequentes a qualquer hora, sem precisar aguardar retorno de um advogado. No Brasil, diversos escritórios implementaram tais soluções para melhorar o relacionamento com os clientes e otimizar o fluxo de trabalho.

Por exemplo, o Assistente Virtual Lexter, voltado ao setor jurídico, realiza triagens iniciais de casos via WhatsApp, coletando informações essenciais do cliente e gerando um resumo para o advogado responsável. Assim, o profissional já recebe o caso previamente estruturado e com indicativos da área de direito pertinente, podendo direcionar seu atendimento de forma mais assertiva. Esse assistente permanece disponível 24 horas por dia, eliminando a necessidade de agendamento de conversas iniciais e permitindo que dúvidas simples sejam resolvidas de imediato.

Além dos escritórios privados, a aplicação de IA conversacional e técnicas correlatas também se destaca no âmbito do Poder Judiciário brasileiro. Um caso emblemático é o Projeto VICTOR, implementado no Supremo Tribunal Federal (STF) em parceria com a Universidade de Brasília.

Embora não seja um “*chatbot*” de atendimento ao público, o Victor funciona como um robô de IA que auxilia na triagem e classificação de recursos judiciais que chegam ao STF.

Antes da introdução dessa ferramenta, a análise de admissibilidade de recursos extraordinários era realizada manualmente por servidores, consumindo tempo valioso. Com o VICTOR, algoritmos de *machine learning* analisam os recursos, identificam o assunto e verificam se se trata de matéria já consolidada pela Corte, agilizando assim a distribuição e a filtragem dos processos.

Desde sua implementação, o projeto contribuiu para acelerar significativamente a tramitação e reduzir o acúmulo de processos no STF, servindo como prova de conceito do potencial da IA em tornar a Justiça mais célere. Outra iniciativa semelhante ocorreu no Superior Tribunal de Justiça (STJ), que adotou o sistema ATHOS para automatizar o exame de admissibilidade de recursos especiais repetitivos.

O ATHOS utiliza IA para identificar processos com questões jurídicas idênticas e agrupá-los conforme temas já decididos ou em julgamento no tribunal. Dessa forma, recursos que tratam de assunto já pacificado podem ser imediatamente direcionados para decisão com base no precedente aplicável, liberando os ministros para se concentrarem nos casos novos ou mais complexos.

Os ganhos incluem celeridade processual (pois evita-se que inúmeros recursos idênticos tramitem separadamente) e uniformização da jurisprudência, já que casos semelhantes recebem tratamento coerente e simultâneo. Vale notar que, embora VICTOR e ATHOS não interajam diretamente com o usuário final como um *chatbot* tradicional, eles representam aplicações práticas da IA no setor jurídico, automatizando tarefas repetitivas de análise textual e tomada de decisão preliminar.

1.2.2 *Chatbots* no Setor Educacional

Na educação, os *chatbots* emergem como ferramentas promissoras para apoiar tanto atividades administrativas quanto pedagógicas. O panorama geral do uso de *chatbots* educacionais indica um crescimento moderado porém constante, com instituições pioneiras já colhendo benefícios, enquanto muitas ainda estudam sua implementação.

No Brasil, uma pesquisa atualizada em 2024 (TÂNGARI, 2024) revelou que 42,4% das 500 maiores instituições de ensino superior do país utilizam algum tipo de chatbot em seus canais de comunicação. Isso significa que cerca de 212 instituições já contam com assistentes virtuais para interagir com alunos ou candidatos, seja em sites, seja em aplicativos de mensagens.

Em contrapartida, 66% das IES avaliadas não utilizavam a ferramenta, evidenciando que há espaço significativo para expansão dessa tecnologia no meio educacional. Muitas das instituições que possuem chats implantados ainda operam de forma básica (sem inteligência artificial ou respostas em tempo real), de modo que o percentual de *chatbots* inteligentes – capazes de compreender e responder automaticamente – corresponde de fato a esses 42,4%.

Observa-se também uma preferência por determinados canais: por exemplo, o WhatsApp desponta como meio favorito para interação automatizada, sendo utilizado em 23% dos casos, seguido de plataformas especializadas integradas a websites institucionais.

Esse cenário mostra que, embora em fase de adoção inicial, os *chatbots* já estão presentes em número considerável de universidades e faculdades brasileiras, particularmente para funções de atendimento ao aluno e marketing educacional. Entre as motivações para sua implantação estão a necessidade de agilizar respostas e a busca por reduzir custos de centrais de atendimento, atendendo a um público estudantil cada vez mais acostumado a soluções digitais instantâneas. De fato, estimativas globais sugerem que o uso de *chatbots* pode gerar economias bilionárias por ano para o setor educacional e outros setores de serviços, além de poupar milhões de horas de trabalho humano ao automatizar tarefas de rotina.

Estudos de caso indicam melhoria significativa nesses processos: no Centro Universitário do Espírito Santo (UNESC), a implementação de um *chatbot* no setor de atendimento acadêmico resultou em aumento de eficiência no atendimento ao público, maior acessibilidade e otimização dos processos internos da universidade.

Uma vantagem inerente é a disponibilidade contínua: os estudantes atuais – nativos digitais – frequentemente realizam pesquisas e tiram dúvidas em horários não

convencionais (madrugada, fins de semana). Com os *bots*, se um potencial aluno acessar o site às 2h da manhã em busca de informação, terá respostas imediatas ou pelo menos o registro de sua solicitação, algo inviável em um modelo de atendimento estritamente humano. Essa prontidão de 24 horas por dia, tende a melhorar a satisfação do usuário e a imagem da instituição como inovadora e orientada ao estudante.

Mais recentemente, os *chatbots* avançaram também para funções pedagógicas diretas, atuando como tutores virtuais inteligentes. Nesse papel, eles podem auxiliar estudantes no aprendizado, esclarecendo conceitos, propondo exercícios e fornecendo feedback personalizado.

Plataformas internacionais de aprendizagem de idiomas, como o Duolingo, incorporaram bots conversacionais que praticam diálogos com o usuário, permitindo que ele treine uma língua estrangeira em qualquer horário.

Empresas como a (JETCHAT, 2025) apontam que a IA na educação pode aumentar a inclusão, pois fornece apoio extra para alunos com necessidades especiais ou dificuldades de aprendizagem, e liberar tempo dos docentes ao automatizar tarefas repetitivas de correção ou esclarecimento de dúvidas básicas.

No Brasil, o surgimento dessas tecnologias gerou debates intensos na comunidade acadêmica em 2023, com pesquisadores ponderando tanto as oportunidades (personalização do ensino, aprendizado adaptativo, democratização do conhecimento) quanto os desafios (plágio, superficialização do estudo, necessidade de letramento digital) de se incorporar IA generativa nas salas de aula. Sem aprofundar nas questões éticas – objeto de outro capítulo deste trabalho –, é possível afirmar que a tendência é de maior convergência entre educação e inteligência artificial nos próximos anos (IFSC, 2023).

As instituições que souberem combinar a expertise humana dos docentes com as capacidades automatizadas dos *chatbots* estarão melhor posicionadas para melhorar a experiência educacional e os resultados de aprendizagem.

1.3 O papel dos dados, *machine learning* no funcionamento da IA

Os dados ocupam uma posição central no contexto da inteligência artificial. Em termos simples, dados são as informações brutas (números, textos, imagens, registros de comportamento etc.) que alimentam os sistemas de IA.

Modelos de IA modernos, especialmente aqueles baseados em *machine learning*, dependem de grandes volumes de dados para extrair padrões e fazer predições acuradas. Nas palavras de Gutierrez (2019), diferentes sistemas de IA – de algoritmos analíticos simples a modelos avançados de *machine learning* – têm em comum que *as questões relacionadas aos dados utilizados [...] são elementares para tais sistemas*.

No processo de treinamento de IA, conjuntos extensos de dados (*datasets*) são utilizados para ensinar o modelo a realizar determinada tarefa. Por exemplo, um sistema de reconhecimento de imagens precisa ser exposto a milhares de fotos rotuladas para aprender a identificar objetos; um chatbot precisa “ler” milhões de frases de diálogos humanos para adquirir fluência linguística. A suficiência e a qualidade desses dados de treinamento são cruciais: dados confiáveis, representativos e livres de vieses conduzem a resultados mais confiáveis, ao passo que dados escassos ou enviesados podem gerar modelos deficientes ou tendenciosos.

Assim, a confiabilidade de um sistema de IA espelha, em grande medida, a confiabilidade e abrangência do conjunto de dados que o alimentou. Esse aspecto é especialmente sensível em aplicações como diagnóstico médico por IA ou recomendações jurídicas automatizadas, nas quais dados incompletos ou distorcidos podem levar a erros graves.

Além do volume, importa considerar a natureza dos dados. Muitos sistemas utilizam dados pessoais, isto é, informações relacionadas a pessoas identificadas ou identificáveis – por exemplo, históricos de compras, interações em redes sociais, localização GPS, conteúdos de mensagens, dentre outros. Esses dados pessoais são frequentemente o “combustível” para algoritmos de recomendação e personalização (como aqueles usados por plataformas de comércio eletrônico ou streaming), bem

como para agentes conversacionais. Isso gera preocupações quanto à privacidade e proteção de dados, tema a ser aprofundado nas próximas seções.

Por ora, ressalte-se que a era do *Big Data* trouxe à IA não apenas poder computacional, mas também dilemas sobre o uso adequado e ético dos dados coletados. As técnicas atuais permitem combinar e cruzar enormes bancos de dados para extrair inferências antes impossíveis, o que confere grande poder preditivo à IA, mas também expõe indivíduos a potenciais violações de privacidade e usos indevidos de suas informações pessoais.

1.3.1 *machine learning* como mecanismo de aprendizagem automatizada

O conceito de *machine learning* (aprendizado de máquina) designa uma categoria de algoritmos de IA que aprendem padrões a partir dos dados, em vez de seguirem instruções programadas explicitamente por humanos.

No *machine learning*, o enfoque se inverte: alimenta-se o algoritmo com exemplos (dados de entrada e saída esperada) e o próprio sistema ajusta internamente seus parâmetros para generalizar um comportamento que se aproxime das respostas corretas.

Além disso, abrange diversas técnicas e abordagens. Em todas essas modalidades, quanto mais dados e experiências o sistema acumula, melhor tende a ser seu desempenho, até certo limite. Um algoritmo supervisionado, por exemplo, precisa de um conjunto robusto de exemplos variados para conseguir generalizar e responder corretamente a casos novos.

Já algoritmos de aprendizado profundo (*deep learning*), que empregam redes neurais artificiais de múltiplas camadas, costumam exigir volumes ainda maiores de dados e poder computacional, mas têm apresentado resultados revolucionários em tarefas complexas como reconhecimento de voz, visão computacional e previsão de linguagem.

Um aspecto importante é que algoritmos de *machine learning* não garantem infalibilidade. Eles aprendem correlações estatísticas nos dados, mas podem falhar em situações fora do padrão ou incorporar vieses presentes no conjunto de treino.

2 FUNDAMENTOS DA RESPONSABILIDADE CIVIL NO DIREITO BRASILEIRO

A responsabilidade civil constitui um dos pilares centrais do ordenamento jurídico privado brasileiro, sendo classificado como o instituto por meio do qual se busca restabelecer o equilíbrio jurídico rompido pela ocorrência de um dano.

Sua premissa fundamental reside na máxima de que a ninguém é lícito causar prejuízo a outrem, impondo ao ofensor o dever de reparar a lesão perpetrada, seja ela de natureza patrimonial ou extrapatrimonial. A disciplina desta matéria não se resume a uma mera técnica de compensação de prejuízos, mas reflete, as escolhas de uma sociedade acerca da distribuição dos ônus e riscos inerentes à convivência e às atividades econômicas.

A compreensão de seus conceitos é indispensável paro o entendimento de sua relação com a IA. Diante de tal relevância, o presente capítulo se dedica a uma análise sistemática dos elementos que estruturam a responsabilidade civil no Brasil. O percurso analítico se iniciará com a exposição das noções gerais e dos pressupostos clássicos que condicionam o surgimento da obrigação de indenizar, notadamente a conduta, o dano, o nexo de causalidade e, em sua vertente tradicional, a culpa.

Posteriormente, a investigação avançará para a distinção entre as modalidades de responsabilidade subjetiva e objetiva, explorando não apenas suas bases teóricas, mas também as implicações práticas decorrentes da adoção de um ou outro regime, o que define a necessidade ou a dispensa da comprovação do elemento volitivo do agente.

Em um terceiro momento, o estudo se voltará para a dimensão contemporânea do instituto, examinando a função social que a reparação civil assume no contexto digital, um ambiente que introduz novos riscos e desafia os paradigmas tradicionais.

Por fim, a análise se aprofundará em um dos microssistemas jurídicos de maior impacto, o Direito do Consumidor, correlacionando a proteção do vulnerável com as teorias do risco do empreendimento e o princípio da boa-fé objetiva.

2.1 Noções gerais e pressupostos da responsabilidade civil

Historicamente, a noção de dano moral já se fazia presente em civilizações antigas, como a Babilônia e Roma. Um dos registros mais antigos sobre a reparação de danos por meio de um sistema legal organizado remonta ao Império Babilônico, durante o governo de Hamurabi (2067–2025 a.C.), onde se estabeleceu um conjunto de leis codificadas que tratavam dessa matéria (REIS, 2010, p. 22). Naquele contexto, predominava a lógica da vingança privada, em que os indivíduos agiam guiados por impulsos primitivos com o intuito de proteger seus próprios interesses.

No Direito Romano, por sua vez, a Lei das Doze Tábuas já previa a punição de atos ilícitos, como a injúria e a difamação, estabelecendo mecanismos de compensação tanto no âmbito penal quanto civil, como se nota na expressão "*iniuriae alii calamo aces XXV*" (REIS, 2010, p. 31). Posteriormente, com a promulgação da Lei Aquília, no século III a.C., houve um avanço importante ao se reconhecer a possibilidade de reparação patrimonial por danos de natureza moral, o que contribuiu para a consolidação do instituto da indenização nesse campo.

Ao longo do tempo, o entendimento sobre o dano moral foi se transformando e se sofisticando, até alcançar o reconhecimento que possui hoje no Direito contemporâneo. No ordenamento jurídico brasileiro, ele encontra respaldo em diversos dispositivos legais, sendo o artigo 186 do Código Civil um dos principais, ao estabelecer que aquele que, por ação ou omissão voluntária, causar dano a outrem, comete ato ilícito. Essa disposição é complementada pelo artigo 927, que prevê a obrigação de reparar o prejuízo causado:

> *"**Art. 186**. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito."*
>
> *"**Art. 927.** Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo.*
>
> ***Parágrafo único**. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem."*

Já a Constituição Federal expressa através do artigo 5, “caput”, incisos V e X, o garantimento do direito da moralidade:

> *"**Art. 5º** Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:*
>
> ***V -** é assegurado o direito de resposta, proporcional ao agravo, além da indenização por dano material, moral ou à imagem;*
> ***X -** são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;"*

Dentro dessa perspectiva, a responsabilidade civil corresponde à obrigação imposta a alguém de reparar prejuízos decorrentes da violação de um dever jurídico, seja essa violação causada por um ato lícito ou ilícito. Essa obrigação está prevista, de forma clara, nos artigos 186 e 927 do Código Civil, que disciplinam o dever de indenizar quando configurado o dano e sua relação com a conduta do agente.

Para que se configure a responsabilidade civil, é necessário o preenchimento de alguns requisitos fundamentais: a conduta (por ação ou omissão), a imputabilidade do agente, a existência de um dano (de natureza material ou imaterial) e o nexo de causalidade entre a conduta e o prejuízo. Tais elementos constituem a base para aferição da responsabilidade. A imputabilidade diz respeito à capacidade do agente responder por seus atos; o dano, por sua vez, representa a lesão efetiva aos bens da vítima, seja no campo patrimonial ou extrapatrimonial; e o nexo causal exige a comprovação de que a conduta do agente foi, de fato, a causa do dano. Há ainda hipóteses que excluem a responsabilidade, como caso fortuito, força maior e culpa exclusiva da vítima.

Podem classificar a responsabilidade civil sob dois eixos principais: quanto à origem da obrigação e quanto à necessidade de demonstração da culpa. Sob o primeiro aspecto, ela pode ser contratual ou extracontratual. A contratual surge do descumprimento de uma obrigação previamente pactuada entre as partes, o que facilita a identificação do responsável pelo dano. Já a responsabilidade extracontratual decorre da violação de dever legal, mesmo na ausência de qualquer vínculo contratual entre as partes.

Já sob o segundo critério, a responsabilidade civil pode ser subjetiva ou objetiva. A subjetiva exige a comprovação de dolo ou culpa para que se possa imputar o dever de indenizar, sendo este o modelo tradicional adotado no direito civil. Por outro lado, a responsabilidade objetiva dispensa a verificação da culpa, bastando a demonstração do dano e do nexo causal. Este modelo é aplicado, por exemplo, nos casos previstos em lei, como nas atividades de risco e nas relações de consumo.

Nesse sentido, o artigo 18 do Código de Defesa do Consumidor é especialmente relevante, pois prevê que, havendo defeito no produto ou serviço que cause dano ao consumidor, este poderá acionar judicialmente qualquer um dos integrantes da cadeia de fornecimento, conforme sua conveniência, o que se coaduna com a lógica da responsabilidade objetiva.

Superada a análise geral da responsabilidade civil, adentra-se à temática do dano moral, que representa uma das formas de reparação mais debatidas atualmente. O dano moral está relacionado à lesão de ordem subjetiva, atingindo valores imateriais do indivíduo, como sua honra, dignidade, intimidade ou equilíbrio emocional. Pode se manifestar de forma “pura” — isto é, reconhecido pela simples ocorrência do ato ilícito ou abusivo, sem necessidade de prova concreta do sofrimento —, ou de forma qualificada, quando é necessário demonstrar que o dano extrapolou os meros aborrecimentos cotidianos e afetou de maneira relevante a esfera pessoal da vítima.

Na atual conjuntura jurídica brasileira, as ações que visam à reparação por danos morais têm se intensificado, evidenciando a valorização dos direitos da personalidade, conforme disposto no artigo 1º, inciso III, da Constituição Federal, que consagra a dignidade da pessoa humana como um dos fundamentos do Estado Democrático de Direito: ″Art. 1º A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito e tem como fundamentos: III - a dignidade da pessoa humana;″, trabalhando em conjunto com o artigo 12 do Código Civil, a respeito da possibilidade de responsabilização civil nos casos em que haja lesão ou perigo de lesão a estes bens jurídicos fundamentais: ″Art. 12. Pode-se exigir que cesse a ameaça, ou a lesão, a direito da personalidade, e reclamar perdas e danos, sem prejuízo de outras sanções previstas em lei.″ ocasionando no dano moral “puro”.

Além das hipóteses em que o entendimento jurisprudencial já consolidou a existência do chamado “dano moral puro” — aquele que prescinde de comprovação do sofrimento —, há situações em que a ofensa não revela de imediato uma violação aos direitos da personalidade. Nesses casos, torna-se indispensável demonstrar a existência de um prejuízo efetivo para que se configure a responsabilidade civil.

No tocante aos contratempos cotidianos, o Enunciado n.º 159 do Conselho da Justiça Federal, aprovado durante a III Jornada de Direito Civil, esclarece que o dano moral não se confunde com os meros aborrecimentos oriundos de perdas materiais. Tais incômodos se inserem no contexto da vida em sociedade e não possuem gravidade suficiente para justificar reparação. Em contraposição, o dano moral indenizável se caracteriza por atingir a esfera íntima do indivíduo, provocando sofrimento relevante e anormal, capaz de abalar o equilíbrio emocional da vítima de forma significativa.

Dado seu caráter subjetivo e intangível, o dano moral possui natureza peculiar no campo da reparação civil. Por não ser possível restituir plenamente o estado anterior da vítima, a compensação assume contornos mais amplos, envolvendo não apenas o aspecto compensatório, mas também o pedagógico e punitivo. O valor fixado a título de indenização deve considerar a extensão do sofrimento experimentado, sem se afastar dos princípios da razoabilidade e da proporcionalidade, funcionando, ainda, como desestímulo à reiteração da conduta lesiva por parte do ofensor.

Assim, a reparação do dano moral deve atender à dupla finalidade: oferecer à vítima uma forma de compensação pelo prejuízo imaterial suportado e, simultaneamente, transmitir à sociedade a reprovação da conduta ilícita, conforme os parâmetros estabelecidos pela legislação vigente e interpretados pelos tribunais, seguindo os preceitos de COELHO, 2009, p. 413: *Há inúmeros argumentos em prol da reparação do dano moral. Os mais relevantes são os seguintes: a) há previsão legal de reparação; b) é preciso proteger o patrimônio imaterial; c) é injusto deixar um dano sem reparação; d) é necessário evitar a prática de condutas anti-sociais; e) a reparação contribui para afastar o uso da autotutela.*

2.2 Responsabilidade objetiva e subjetiva: distinções teóricas e práticas

Em sede de responsabilidade civil, a distinção entre a responsabilidade subjetiva (calcada na culpa) e a objetiva (independente de culpa) é fundamental. No modelo clássico subjetivo, consagrado no art. 186 do Código Civil, exige-se a comprovação de conduta culposa ou dolosa do agente: “Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito”.

Ou seja, a culpa (*lato sensu*) – englobando negligência, imprudência ou imperícia – é pressuposto para o dever de indenizar. Por outro lado, na responsabilidade objetiva a reparação independe de indagação sobre culpa ou dolo.

O próprio Código Civil de 2002, além de prever a regra geral subjetiva, adotou expressamente a cláusula geral da responsabilidade objetiva em seu art. 927, parágrafo único, dispondo que “haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem”.

Trata-se da consagração da chamada teoria do risco, segundo a qual aquele que exerce atividades por natureza arriscadas ou lucrativas deve arcar com os prejuízos delas decorrentes, ainda que aja sem culpa. Nas palavras de renomada doutrina, a responsabilidade objetiva visa a proteger melhor a vítima, distribuindo os custos do dano a quem realiza a atividade e dela extrai benefício (DINIZ, 2010, p. 73).

Assim, enquanto a responsabilidade subjetiva fundamenta-se na culpa provada do agente, a responsabilidade objetiva funda-se no risco da atividade e em determinações legais específicas, dispensando a prova de culpa e bastando a relação de causalidade entre a conduta (ou atividade) e o dano (GONÇALVES, 2017, p. 35).

Do ponto de vista teórico, a responsabilidade subjetiva enfatiza a ideia de reprovabilidade da conduta individual – somente se pune civilmente quem agiu com má-fé, negligência ou imprudência. Já a objetiva enfatiza a proteção da vítima e os riscos do empreendimento: presume-se a responsabilidade de quem cria o risco,

ainda que tenha atuado com toda a cautela possível. Na prática, isso implica diferenças probatórias e de política jurídica.

Pelo regime subjetivo tradicional, o lesado deve demonstrar a falha ou omissão do fornecedor de informação (por exemplo, a empresa de tecnologia não programou ou supervisionou adequadamente o *chatbot*, ou atuou com negligência na atualização de seus dados). Sob o regime objetivo, por sua vez, basta evidenciar que a informação equivocada/fraudulenta foi fornecida pelo serviço do fornecedor e causou dano ao consumidor, sendo desnecessário investigar minúcias da conduta interna da empresa.

Como ressaltam Pablo Stolze e Rodolfo Pamplona, o ordenamento passou a conviver com dois modelos: um regime subjetivo comum, baseado na culpa, e um regime objetivo especial, aplicável em situações previstas em lei ou marcadas por riscos exacerbados, visando à tutela mais eficiente das vítimas (STOLZE; PAMPLONA, 2014, p. 58-59).

Atualmente, diversas legislações específicas adotam a responsabilidade objetiva – a exemplo do Código de Defesa do Consumidor (Lei 8.078/90) no tocante aos defeitos do serviço e do produto, e da própria Lei Geral de Proteção de Dados (Lei 13.709/18) no tocante a danos causados pelo tratamento ilícito de dados pessoais.

Essas normas refletem uma opção clara do legislador brasileiro pela teoria do risco e pela distribuição equitativa dos ônus dos danos advindos da atividade econômica, especialmente em contextos de assimetria entre fornecedor e consumidor.

Quando se transpõem essas distinções para o contexto dos *chatbots* de inteligência artificial (IA) e sua atuação no fornecimento de informações ao público, emergem desafios peculiares (CASEIRO, 2019, p. 139). Por um lado, pode ser difícil imputar culpaindividual a um agente humano específico, já que as respostas e decisões do *chatbot* resultam de algoritmos complexos e bases de dados amplas, frequentemente operando de forma autônoma.

Diante do déficit de imputação subjetiva, ganha força a aplicação da responsabilidade objetiva: ao invés de buscar uma culpa difícil de comprovar, presume-se a responsabilidade do fornecedor da tecnologia com base no risco

inerente à atividade de atendimento automatizado. Afinal, o desenvolvimento e fornecimento de *chatbots* integra a atividade econômica da empresa de tecnologia – atividade esta que, por sua natureza, pode acarretar riscos aos direitos dos consumidores (como o risco de desinformação, fraudes eletrônicas, indução a erro etc.).

Aplica-se aqui o já referido art. 927, parágrafo único, do CC, bem como os preceitos do direito do consumidor, atribuindo-se ao fornecedor o dever de responder por informações enganosas ou falhas oriundas do sistema de IA, independentemente de ter havido intenção ou negligência identificável. Em outros termos, o risco do empreendimento recai sobre o empresário, não sobre a parte vulnerável (VENOSA, 2013, p. 37).

Essa orientação objetiva não exclui, por óbvio, a apuração de condutas dolosas específicas – por exemplo, se ficar demonstrado que a empresa programou deliberadamente o chatbot para enganar usuários (dando informações fraudulentas para obter vantagem), estar-se-á diante de ilícito com culpa grave ou dolo, o que reforça ainda mais o dever de indenizar pelo regime subjetivo clássico.

Todavia, nos casos mais comuns de informações equívocas involuntárias geradas pelo algoritmo (as chamadas "*alucinações*" da IA, em que o sistema fornece dados falsos crendo serem verdadeiros), a vítima não ficará desamparada: poderá invocar a responsabilidade objetiva do fornecedor.

Em suma, do ponto de vista prático e teórico, a distinção entre responsabilidade subjetiva e objetiva traduz diferentes caminhos para assegurar a reparação civil.

No contexto da inteligência artificial aplicada ao atendimento automatizado, essa distinção revela também uma escolha de política jurídica: ou se exige da vítima a prova da falha humana específica por trás da máquina – hipótese que pode levar à inexigibilidade da reparação por ausência de culpa comprovada –, ou se imputa diretamente à empresa que explora a tecnologia o custo dos danos causados ao consumidor, com base no risco assumido e na tutela do hipossuficiente.

O ordenamento brasileiro, amparado tanto na doutrina quanto na legislação, inclina-se por esta segunda via em situações análogas, garantindo maior segurança jurídica e proteção ao lesado.

2.3 A função social da reparação civil no contexto digital

A responsabilidade civil não se destina unicamente a recompor o prejuízo individual da vítima; ela cumpre também uma função social ampla. A Constituição Federal de 1988, já em seu art. 5º, assegura o direito à indenização por danos morais e materiais decorrentes de violações de direitos fundamentais (honra, imagem, intimidade etc.), reconhecendo a reparação civil como instrumento de tutela da dignidade da pessoa humana.

Essa orientação constitucional sinaliza que a reparação de danos possui um papel que transcende o interesse privado das partes envolvidas, atendendo a imperativos maiores de justiça e equilíbrio social. Delineia-se a ideia de que a responsabilidade civil moderna desempenha três funções básicas: (i) a função compensatória, voltada a indenizar o lesado pelos danos sofridos; (ii) a função punitiva ou sancionatória do lesante (embora de maneira branda no ordenamento brasileiro, que não adota penas civis expressivas, admite-se certo caráter punitivo nos danos morais, por exemplo); e (iii) a função preventiva/pedagógica, pela qual o dever de indenizar atua como fator de desestímulo a comportamentos lesivos e de incentivo a medidas de cautela.

A essa tríade soma-se a chamada função social da responsabilidade civil, destacada por autores como Maria Helena Diniz e Sílvio Venosa, que consiste em alinhar o instituto da reparação com os valores coletivos e os fins sociais da lei (DINIZ, 2010, p. 66; VENOSA, 2013, p. 45).

Em outras palavras, ao impor a reparação de um dano, o Direito busca não apenas fazer justiça no caso concreto, mas também influenciar positivamente o meio social, prevenindo novos danos e reforçando deveres de solidariedade e respeito mútuo nas relações.

No contexto digital, a função social da responsabilidade civil ganha contornos ainda mais relevantes. Vivemos a era dos fluxos massivos de informação e dos serviços automatizados, em que empresas de tecnologia coletam e processam dados de milhões de usuários e influenciam diretamente o modo como consumimos informação e interagimos.

A reparação civil, nesse cenário, torna-se um instrumento de *accountability* das atividades digitais: cada condenação ou acordo indenizatório em razão de falhas de um serviço automatizado sinaliza para o mercado que determinados padrões de conduta são exigíveis em prol da coletividade. Socialmente, a existência de responsabilidade civil robusta no âmbito das novas tecnologias contribui para elevar os padrões de segurança e qualidade dos serviços digitais.

Por exemplo, se *chatbots* bancários ou de saúde – utilizados para orientar consumidores – estiverem sujeitos a gerar responsabilidade por informações equívocas que causem prejuízo financeiro ou risco à saúde, as empresas provedoras serão incentivadas a investir em mecanismos de validação das respostas, em treinamento das IAs para minimizar erros (redução de outputs enganosos) e em fornecimento de avisos claros aos usuários sobre eventuais limitações do serviço.

A reparação de um dano individual cumpre, assim, um papel pedagógico amplo: educa o fornecedor e o mercado quanto à necessidade de diligência e boa-fé, e tranquiliza a coletividade de que há proteção jurídica caso haja falhas. Trata-se de assegurar, em última instância, a confiança dos cidadãos no uso das novas ferramentas digitais, condição indispensável para o pleno desenvolvimento social e econômico no ambiente virtual.

Nas lições de Carlos Roberto Gonçalves, a evolução da responsabilidade civil incorpora preocupações coletivas e difusas – como a segurança dos consumidores em massa e o respeito aos direitos da personalidade diante de tecnologias invasivas – de modo que a reparação civil atua como verdadeiro instrumento de pacificação social e de realização dos valores constitucionais no dia a dia tecnológico (GONÇALVES, 2018, p. 17-19).

Um aspecto particularmente importante da função social da responsabilidade civil no meio digital é o contrapeso ao poder tecnológico das empresas. Grandes plataformas e provedoras de sistemas de IA frequentemente impõem aos usuários contratos de adesão e termos de uso extensos, que visam limitar ao máximo sua responsabilidade.

Shoshana Zuboff, ao estudar o chamado capitalismo de vigilância, destaca que as big techs vêm explorando brechas legais e a passividade dos usuários para consolidar um regime privado de exceção, no qual conseguem subtrair direitos do consumidor por meio de cláusulas unilaterais.

Zuboff relata que esses contratos digitais de adesão funcionam como uma espécie de "*domínio eminente privado*", isto é, uma apropriação unilateral de direitos sem o devido consentimento, uma verdadeira "*degradação moral e democrática do domínio da lei e da instituição do contrato, uma perversão que reestrutura os direitos dos usuários concedidos mediante processos democráticos, substituindo-os pelo sistema que a empresa deseja impor*" (ZUBOFF, 2020, p. 265).

Tal diagnóstico evidencia que, na ausência de freios, o desequilíbrio entre empresas de tecnologia e consumidores pode minar conquistas jurídicas básicas. É nesse ponto que a responsabilidade civil exerce uma função social corretiva: ao garantir que, não obstante os termos contratuais abusivos ou a complexidade tecnológica, o lesado terá direito a reparação, reforça-se a supremacia dos princípios legais sobre as vontades unilaterais das corporações.

Em outras palavras, a perspectiva social da reparação recoloca a proteção da pessoa em primeiro plano, lembrando que o desenvolvimento tecnológico deve submeter-se aos valores de dignidade humana, confiança e lealdade nas relações.

A própria LGPD – Lei Geral de Proteção de Dados – explicita entre seus fundamentos tanto a inovação e a livre iniciativa quanto a defesa do consumidor e os direitos humanos, sinalizando que o ordenamento busca um ponto de equilíbrio: incentiva-se o progresso tecnológico, porém sem abdicar da proteção dos cidadãos.

A responsabilização civil de empresas de IA que causem danos insere-se nesse equilíbrio, funcionando como garantia de que a inovação digital atenda à sua função

social – isto é, que sirva ao bem-estar das pessoas e não apenas aos interesses econômicos dos fornecedores.

Por fim, é importante destacar que a função social da responsabilidade civil no âmbito digital também engloba a ideia de prevenção e combate a ilícitos tecnológicos difusos. A *Internet* amplificou problemas como a desinformação em massa (fake news), fraudes cibernéticas e violações de privacidade. Muitas vezes, tais práticas lesivas envolvem o uso de algoritmos ou plataformas automatizadas.

A reparação civil, nesses casos, pode ter caráter coletivo (ações civis públicas, danos morais coletivos) buscando não apenas compensar prejuízos difusos, mas sinalizar um padrão de conduta socialmente desejável. Assim, a condenação de uma empresa cujo *chatbot* disseminou informações enganosas ou discriminatórias, por exemplo, presta-se também a afirmar valores caros à sociedade – a veracidade, a igualdade, a não discriminação – e a educar os demais atores do mercado digital quanto às consequências de práticas irresponsáveis.

Em síntese, a responsabilidade civil, ao cumprir sua função social no contexto da inteligência artificial e do atendimento automatizado, atua como garantia institucional de que os avanços tecnológicos serão acompanhados de responsabilidade jurídica. Por meio dela, efetiva-se o mandamento constitucional de construir uma sociedade livre, justa e solidária, na qual o desenvolvimento da tecnologia da informação esteja a serviço dos direitos fundamentais e da confiança pública, e não como instrumento de impunidade ou abuso.

2.4 A proteção do consumidor, o risco do empreendimento e a boa-fé objetiva

No Brasil, a proteção do consumidor é alçada à categoria de princípio constitucional. O art. 5º, inc. XXXII, da Constituição determina que “o Estado promoverá, na forma da lei, a defesa do consumidor”, e o art. 170, inc. V, inclui a defesa do consumidor entre os princípios da ordem econômica. Esse respaldo constitucional se materializou na Lei 8.078/1990 – o Código de Defesa do Consumidor (CDC) – que estabelece um microssistema jurídico fortemente protetivo da parte mais vulnerável nas relações de consumo. Três pilares desse sistema revelam-se

particularmente pertinentes diante do tema da responsabilidade civil por informações errôneas fornecidas via *chatbots* de IA: (i) a responsabilidade objetiva do fornecedor (teoria do risco do empreendimento); (ii) o direito à informação; e (iii) o princípio da boa-fé objetiva nas relações de consumo.

Conforme o CDC, o fornecedor de produtos ou serviços responde independentemente de culpa pelos vícios e defeitos desses bens ou serviços. O art. 14 do CDC dispõe que o fornecedor de serviços "*responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos*".

Tem-se aqui a consagração expressa da teoria do risco do empreendimento: se uma empresa se dispõe a colocar um serviço no mercado – por exemplo, um sistema de atendimento automatizado por chatbot – ela assume os riscos inerentes a essa atividade e deve arcar com os prejuízos derivados de falhas do serviço, ainda que não tenha agido com intenção ou negligência.

A ideia subjacente, bem sintetizada por Silvio Venosa, é a de que "*o custo dos danos integra o custo do negócio*", de modo que o fornecedor (que aufere lucro com a atividade) deve internalizar esse custo em vez de repassá-lo ao consumidor individualmente lesado (VENOSA, 2017, p. 37).

No âmbito de informações equívocas ou enganosas fornecidas por *chatbots*, não há dúvida de que se trata de um defeito do serviço de atendimento, pois o resultado esperado (informação correta e útil) não foi entregue adequadamente, causando prejuízo ao consumidor.

Pela legislação consumerista, pouco importa averiguar se houve falha humana no desenvolvimento do algoritmo ou se a empresa poderia ter evitado o erro específico – basta que o serviço, considerado em si mesmo, mostrou-se defeituoso em sua função de informar, para surgir o dever de indenizar.

Essa orientação objetiva facilita e viabiliza a tutela do consumidor em face de gigantes da tecnologia: o consumidor não precisa desvendar a caixa-preta do algoritmo para provar uma falha oculta ou má programação; ao contrário, cabe à

empresa demonstrar, se for o caso, alguma excludente de responsabilidade prevista em lei (por exemplo, culpa exclusiva da vítima ou de terceiro, o que em contexto de *chatbots* seria bastante inusual).

Vale ressaltar que mesmo a nova LGPD – ao tratar da responsabilização de controladores e operadores de dados – adotou estrutura semelhante à do CDC, prevendo responsabilidade solidária e inversão do ônus da prova em benefício do titular lesado. Isso evidencia uma convergência normativa no sentido de atribuir às empresas de tecnologia o ônus jurídico por riscos do ambiente digital, coerente com a proteção do consumidor e do cidadão usuário.

Em suma, pelo prisma do risco do empreendimento, a empresa fornecedora de *chatbots* responde objetivamente pelos danos que seus sistemas causem – seja um erro informativo que leve o consumidor a um prejuízo financeiro, seja uma orientação defeituosa que gere um dano à saúde ou segurança do usuário.

A tutela do consumidor, assim, prevalece sobre eventuais cláusulas de não garantia ou termos de uso que busquem eximir totalmente a responsabilidade do fornecedor (conforme o art. 51 do CDC, são nulas de pleno direito, cláusulas contratuais que pretendam exonerar o fornecedor de responder por vícios ou danos ao consumidor, por afrontarem a boa-fé e a ordem pública do consumo).

Outro aspecto crucial é o direito à informação adequada, clara e verdadeira, assegurado como direito básico do consumidor (art. 6º, III, CDC). Quando o atendimento é realizado por uma inteligência artificial, não se exime a empresa do dever de fornecer informações corretas sobre produtos, serviços ou sobre si mesma.

Se um *chatbot* prestar uma informação incompleta, confusa ou objetivamente falsa – por exemplo, induzir o consumidor a acreditar que certo produto possui características que não tem, ou que determinada operação bancária não acarreta tarifas quando na verdade acarreta – esse dever legal é violado.

A consequência, além das sanções administrativas cabíveis, recai na esfera civil: configura-se o dano ao direito do consumidor, passível de reparação, e também o nexo causal entre a conduta (informação defectiva) e o prejuízo sofrido (decisão equivocada do consumidor baseada na informação incorreta). Aqui, o elemento

informativo é central na relação de consumo, de modo que a veracidade e transparência das interações "*homem-máquina*" devem ser equiparáveis às que seriam exigidas de um atendente humano.

Em outras palavras, a empresa não pode escudar-se no argumento de que o robô detém a responsabilidade pelo o que disse, e não a empresa.

Pode-se dizer que o *chatbot* é extensão da pessoa jurídica fornecedora, e tudo que ele comunica ao público, no contexto da relação de consumo, é atribuído à empresa. Essa atribuição se dá não apenas por força da lei, mas também pela lógica do princípio da boa-fé objetiva.

A boa-fé objetiva consiste num padrão ético-jurídico de comportamento leal, transparente e cooperativo que deve permear todas as fases das relações contratuais e de consumo. Prevista no Código Civil (art. 422, obrigando os contratantes a observarem os princípios de probidade e boa-fé na conclusão e execução dos contratos) e reafirmada no CDC (art. 4º, III, que orienta a política nacional das relações de consumo pela boa-fé e equilíbrio entre as partes), essa boa-fé impõe deveres anexos como o dever de informação, de não fraude, de proteção e lealdade.

No caso das empresas de tecnologia que operam *chatbots*, boa-fé objetiva significa, por exemplo, o dever de programar o atendimento automatizado de forma honesta – sem inserir algoritmos que deliberadamente manipulem ou enganem o consumidor – e o dever de corrigir prontamente eventuais erros graves de informação dos quais tenham ciência.

Também implica a obrigação de alertar o usuário sobre limites do sistema: agir com boa-fé é, por exemplo, informar claramente se as respostas do assistente virtual são meramente automatizadas e podem conter falhas, ou disponibilizar fácil acesso a um atendente humano quando a complexidade do assunto superar as capacidades do *bot*.

Por outro lado, se a empresa utiliza o *chatbot* para induzir o consumidor em erro (imaginemos um cenário em que o robô de vendas omite informações importantes ou enfatiza apenas pontos que favorecem o fornecedor, levando o consumidor a contratar

um serviço desvantajoso), tem-se uma violação clara da boa-fé objetiva e do dever de informação.

Nesse caso, além da anulabilidade do negócio ou outras consequências, haverá responsabilidade civil pelos danos causados. Mesmo na hipótese em que o equívoco informativo não seja proposital, a boa-fé objetiva requer da empresa uma postura diligente ao tomar conhecimento do erro: ocultar a falha, ou deixar diversos consumidores lesados sem esclarecimentos, reforçaria o descumprimento desse dever de lealdade.

Cabe salientar que a boa-fé objetiva serve de critério para interpretar e integrar contratos e relações jurídicas; assim, em eventual processo, a conduta da empresa de tecnologia será julgada à luz do comportamento que dela se esperava conforme os padrões de confiança.

A utilização de IAs não exime – ao contrário, pode até ampliar – a expectativa social de que uma empresa haja com transparência e corrija distorções. Afinal, quem detém o controle (ainda que indireto) sobre algoritmos complexos está em posição privilegiada para saber de seus riscos e deve adotar todas as medidas razoáveis para prevenir danos a terceiros, sob pena de infringir a rule of thumb da confiança mútua.

Em termos práticos, a articulação entre proteção do consumidor, risco do empreendimento e boa-fé objetiva conduz a um regime de responsabilidade civil bastante protetivo no tocante a *chatbots* e sistemas de atendimento automatizado.

O consumidor que recebe uma informação fraudulenta ou equivocada e sofre prejuízo tem ao seu favor: (i) a responsabilidade objetiva do fornecedor (não sendo necessário provar culpa, apenas o defeito do serviço e o dano); (ii) o direito básico à informação violado, que por si só já caracteriza ilícito; e (iii) a presunção de que houve quebra da boa-fé e do dever de confiança na relação, reforçando o dever de indenizar.

A empresa, por sua vez, só poderá eximir-se se demonstrar alguma causa excludente robusta, como, por exemplo, que o erro decorreu unicamente de um hacker ou ato de terceiro totalmente alheio ao seu controle (hipótese rara, que não afasta a possível *culpa in vigilando* da própria empresa).

Em última análise, o ordenamento jurídico, ao imputar às empresas de tecnologia o ônus pelos riscos de sua atividade e ao exigir delas conduta proba e transparente, busca equiparar e equilibrar a relação fornecedor-consumidor no ambiente digital. Isso se coaduna com a visão de que a inovação deve respeitar direitos: não por acaso, a LGPD elenca entre seus fundamentos tanto o incentivo ao desenvolvimento tecnológico quanto a defesa do consumidor e a dignidade humana, lado a lado.

Em outras palavras, reconhece-se que livre iniciativa e boa-fé objetiva devem caminhar juntas. A firma que inova oferecendo um chatbot sofisticado obtém ganhos de eficiência e lucro, mas em contrapartida assume um dever jurídico de responder por eventuais malefícios dessa inovação, observando sempre a confiança depositada pelo público consumidor em seus serviços.

Somente assim se concretiza o mandamento constitucional de proteção ao consumidor na era da inteligência artificial, garantindo que a adoção massiva de sistemas automatizados de informação não resulte em terra sem lei, mas sim em um círculo virtuoso de inovação responsável: empresas conscientes de seus deveres, consumidores amparados em seus direitos, e o Direito servindo de guia para uma tecnologia mais ética e alinhada com o interesse público.

3 EMPRESAS DE TECNOLOGIA E OS DEVERES INFORMATIVOS

A digitalização das relações econômicas e sociais instaurou uma nova forma de vivência caracterizado por uma assimetria informacional entre os fornecedores de tecnologia e seus usuários.

A complexidade inerente aos sistemas algorítmicos, às plataformas digitais e às soluções de IA confere às empresas detentoras dessas tecnologias um poder significativo, derivado não apenas do controle sobre a infraestrutura, mas sobre o fluxo e o processamento de informações. Essa disparidade de conhecimento e controle cria uma vulnerabilidade estrutural para consumidores e clientes, tornando a informação um elemento central para o reequilíbrio de poder e para a garantia de decisões livres e conscientes.

Em resposta a esse cenário, o ordenamento jurídico impõe às empresas de tecnologia um conjunto robusto de deveres informativos, que se desdobram dos princípios da transparência, da boa-fé objetiva e da confiança. Tais deveres não se esgotam na mera prestação de informações sobre produtos e serviços, mas se estendem à necessidade de garantir o bom funcionamento dos sistemas, os critérios utilizados em decisões automatizadas e os riscos associados ao uso da tecnologia.

O presente capítulo se propõe a analisar a natureza e a extensão desses deveres no contexto tecnológico. A investigação terá início com uma abordagem sobre o dever de informar nas relações de consumo mediadas pela tecnologia, um dos pilares do Código de Defesa do Consumidor.

Em seguida, o foco se deslocará para as obrigações legais e os princípios contratuais especificamente aplicáveis aos fornecedores de IA. A análise se aprofundará nos conceitos de transparência algorítmica e accountability empresarial, discutindo os mecanismos necessários para tornar os sistemas de IA mais inteligíveis e seus desenvolvedores mais responsáveis.

Por fim, serão examinados os riscos inerentes à automação e os limites do controle humano sobre os outputs informacionais, questionando até que ponto é possível garantir uma supervisão efetiva e atribuir responsabilidade em ambientes operados por sistemas crescentemente autônomos.

3.1 O dever de informar nas relações de consumo mediadas por tecnologia

No direito brasileiro, o dever de informar é fundamento do Código de Defesa do Consumidor (CDC), consagrado no artigo 6º, inciso III, como expressão do princípio da transparência. Esse dever tem por objetivo permitir ao consumidor escolhas conscientes, baseadas em dados claros, precisos e adequados sobre produtos e serviços. Todavia, as relações de consumo mediadas por tecnologias digitais ampliam a assimetria informacional tradicional.

Vettorazzi e Bottini, 2025, p. 4-6, a chamada vulnerabilidade digital do consumidor deriva da dificuldade de compreender sistemas algorítmicos complexos que orientam sua navegação e suas decisões de consumo. Em outras palavras, interfaces opacas e contratos eletrônicos extensos rompem com o modelo clássico de oferta: termos de uso prolixos e linguagem técnico-jurídica são aceitos automaticamente, criando um paradoxo entre o dever legal de transparência e informações efetivamente ininteligíveis ao usuário. Esse fenômeno, já descrito como "*choque informacional*" (SOLOVE, 2021, p. 85-87, converte a oferta de informação em mera formalidade, restringindo a autodeterminação do consumidor.

MARQUES, 2023, p. 5 propõe reconhecer a vulnerabilidade digital como nova categoria normativa para o CDC. Ela destaca que termos de adesão, políticas de privacidade e "*dark patterns*" manipulativos submetem o consumidor a uma assimetria radical, pois este não apenas ignora as condições contratuais, mas é influenciado silenciosamente por técnicas de persuasão algorítmica.

Ademais, PASQUALE, 2015, 60-61 complementa essa análise ao caracterizar nossa era como uma "*sociedade da caixa-preta*", em que decisões automatizadas operam sem prestação de contas, deslocando o controle informacional de indivíduos para grandes corporações tecnológicas.

Assim, o dever de informar, concebido como instrumento de emancipação do consumidor, perde eficácia quando inserido em ambientes informacionais opacos e manipulativos. A mera disponibilização formal de termos de uso e políticas de

privacidade não satisfaz o princípio da transparência quando opera em sistemas além do alcance de compreensão do cidadão comum.

Diante desse cenário, a doutrina contemporânea aponta para a necessidade de reinterpretar o dever de informação em termos substantivos, não somente formais. Propõe-se que o conteúdo informacional seja repensado por meio de designs acessíveis, linguagem simplificada e recursos didáticos (como infográficos interativos), de modo a tornar claras as lógicas algorítmicas subjacentes às ofertas e decisões digitais.

A Lei Geral de Proteção de Dados (LGPD) já introduziu avanços ao prever, em seu art. 9º, o direito do titular de dados a obter do controlador informações claras, adequadas e ostensivas sobre critérios e procedimentos de tratamento, inclusive automatizado.

No entanto, esse direito ainda enfrenta obstáculos práticos — baixa literacia digital e complexidade técnica — que aprofundam a vulnerabilidade do consumidor digital.

Em suma, na era digital é urgente uma reformulação normativa e pedagógica do dever de informar, incorporando princípios de explicabilidade algorítmica e fomentando a educação digital crítica, para que a transparência deixe de ser mero formalismo e se torne compreensível e efetiva.

3.2 Obrigações legais e princípios contratuais aplicáveis aos fornecedores de IA

Os fornecedores de soluções baseadas em inteligência artificial (IA) atuam, em regra, como fornecedores no âmbito do CDC quando seus produtos ou serviços são destinados ao consumidor final. Isso implica que estão submetidos às mesmas obrigações gerais de transparência e informação previstas no CDC. Por exemplo, o art. 31 do CDC impõe que "a oferta e apresentação de produtos ou serviços devam assegurar informações corretas, claras, precisas, ostensivas e em língua portuguesa sobre suas características, qualidades, composição, preço, garantia, prazos de validade e origem”. Tal dispositivo exige do fornecedor de IA a descrição adequada

do funcionamento e dos riscos de suas tecnologias, sob pena de violar o direito básico do consumidor à informação.

Ademais, segundo Miragem e Kretzmann, todo dever de informar no direito do consumidor funda-se na boa-fé objetiva e na tutela da confiança do consumidor. Ou seja, espera-se do fornecedor de IA um comportamento proativo e leal em comunicar as limitações e consequências do uso de sistemas automatizados.

No âmbito contratual, muitas soluções de IA são disponibilizadas através de contratos eletrônicos de adesão (termos de uso ou licenças de software). Mesmo nesses contratos massificados, vigoram os princípios contratuais do direito civil e do CDC: as cláusulas não podem violar a função social do contrato nem a boa-fé objetiva (arts. 421, 422 do CC), nem podem impor obrigações abusivas que desequilibrem injustamente as partes.

Ainda que o fornecedor especifique termos de uso, estes devem ser redigidos em linguagem acessível e verossímil, sob pena de serem considerados vexatórios ou nulos. Não obstante, a prática mostra que tais contratos frequentemente reproduzem assimetrias – hipótese em que o CDC permite a revisão judicial da relação e a aplicação de cláusulas gerais (art. 6º, IV do CDC).

Além do CDC, os fornecedores de IA lidam necessariamente com dados pessoais, sendo classificados como controladores ou operadores na LGPD. A LGPD impõe princípios e obrigações específicos: os dados pessoais devem ser tratados de forma transparente, finalista, minimizada e segura (arts. 6º, 7º e 8º da LGPD).

Em especial, o art. 9º da LGPD assegura ao titular o direito de informações claras e ostensivas do controlador sobre critérios e procedimentos de decisão automatizada. Ou seja, o fornecedor de IA deve garantir relatórios ou explicações sobre os algoritmos que processam dados de usuários. No plano contratual, isso se traduz em fornecer, sempre que pertinente, cláusulas específicas de consentimento e informações sobre fins e bases legais do tratamento.

Ademais, o princípio da *accountability* (responsabilização) contido no art. 6º, §1º da LGPD impõe ao controlador comprovar a adoção de políticas eficazes de governança e segurança da informação.

Por fim, vale destacar que o Código Civil brasileiro e a jurisprudência reconhecem a responsabilidade objetiva dos fornecedores em relações de consumo. Isso significa que, em caso de dano causado por software de IA (erro de algoritmo, falha de segurança etc.), o fornecedor responde independentemente de culpa.

Essa obrigação amplificada de cuidado impõe aos desenvolvedores de IA o dever constante de aperfeiçoar seus sistemas, mitigar riscos e alertar o usuário sobre eventuais limitações. Conjugando os princípios contratuais – como equidade e lealdade – com a rigorosa tutela do consumidor, observa-se que empresas de tecnologia devem pautar-se por padrões elevados de transparência e diligência ao fornecer IA, sob pena de configurar omissão injustificável no dever de informar.

3.3 Transparência algorítmica e *accountability* empresarial

A transparência algorítmica consiste na capacidade de explicação das lógicas e critérios subjacentes às decisões automatizadas. Ela é crucial para que usuários e reguladores entendam como sistemas de IA operam e quais parâmetros influenciam seus resultados.

Como nota, GAMBA, 2023, p. 1-15, a transparência algorítmica é “essencial para explicar as decisões automatizadas, mitigar vieses e promover a confiança na tecnologia”. Na prática, isso significa que empresas devem documentar e expor de forma inteligível os procedimentos de análise de dados e inferências que levam a uma recomendação ou decisão – por exemplo, a aprovação de um empréstimo ou a priorização de conteúdo em redes sociais. Sem essa explicabilidade, soluções de IA tornam-se “*caixas-pretas*” que frustram o direito do usuário de contestar ou compreender resultados que lhe afetam, minando sua autonomia de escolha.

O princípio da *accountability* empresarial – adotado em normas internacionais (como o GDPR europeu) e consagrado na LGPD – complementa a transparência.

Em síntese, *accountability* exige que a empresa publique contas sobre seus processos: isto inclui a realização de avaliações de impacto, auditorias independentes e a indicação de responsáveis pela governança dos algoritmos. Eesse princípio surge

como a abertura dos procedimentos de tomada de decisão sobre o que será considerado um risco.

Em outras palavras, à medida que decisões automatizadas envolvem tratamento de dados pessoais, é necessário um marco de regulação baseado na análise de riscos e na prestação de contas dos agentes. A empresa de tecnologia, portanto, deve estar preparada para demonstrar aos órgãos reguladores (e ao público) as medidas de *compliance* que adotou, desde a seleção de bases de dados até o monitoramento de saídas do algoritmo.

Nesse contexto, iniciativas como relatórios de impacto e governança interna de IA contribuem para concretizar a *accountability* e assegurar que a automação não ocorra sem a devida supervisão.

Ademais, entende-se que a eficácia da transparência e da *accountability* depende de respaldo legal claro. Como nota, GAMBA, 2023, p. 6-7, “a legislação pode estabelecer diretrizes claras sobre a transparência na tomada de decisões algorítmicas, responsabilizando as instituições e promovendo a prestação de contas por eventuais danos causados”. Assim, se um sistema de IA causar prejuízo (por erro de análise ou viés injusto), a empresa responsável não poderá alegar ignorância sobre seus próprios processos: ela foi incumbida pelo ordenamento jurídico de clarificar publicamente seu funcionamento.

Em suma, a interação entre transparência algorítmica e *accountability* cria um duplo mecanismo de controle: os consumidores exigem explicações inteligíveis, enquanto o Estado exige documentações e demonstrações de conformidade. Essa dupla dimensão reforça a governança corporativa da IA e alinha o uso tecnológico aos direitos fundamentais dos indivíduos.

3.4 Riscos da automação e os limites do controle humano sobre os outputs informacionais

A automação intensiva das relações de consumo traz ganhos de eficiência, mas também acarreta riscos significativos aos consumidores e à própria sociedade. Como

constatam MANZATO, 2025, p. 12-13 embora IA e contratos digitais aumentem a produtividade, "*também representam riscos à privacidade, honra e imagem, exigindo mecanismos de controle e transparência*". Decisões automatizadas podem introduzir falhas ou vieses que dificilmente seriam previstos por um agente humano isoladamente. Por exemplo, sistemas de recomendação podem perpetuar discriminações existentes na base de dados, e modelos preditivos mal calibrados podem negar crédito ou benefícios indevidamente. A falta de supervisão humana adequada pode impedir a correção dessas falhas em tempo hábil.

Esse cenário evidencia a perda parcial de controle humano sobre as próprias criações: à medida que algoritmos aprendem e evoluem, torna-se mais difícil prever e compreender cada output informacional.

Além disso, a rigidez de contratos eletrônicos de adesão agrava o problema. Cláusulas abusivas ou excludentes de responsabilidade, muitas vezes ocultas, podem eximir o fornecedor de reparação por resultados danosos ou imprevistos gerados pela IA. Ainda que a responsabilidade objetiva do fornecedor cubra danos ao consumidor, na prática resta debate sobre quem, exatamente, responde quando um algoritmo "*erra*" – o desenvolvedor original do software, o fornecedor do serviço ou mesmo o próprio usuário que definiu parâmetros da automação.

Em âmbito civil, estudos recentes apontam que, no Brasil, a responsabilização por IA segue a teoria do risco: por analogia ao art. 927 do Código Civil, o desenvolvedor, proprietário ou usuário do sistema de IA poderá ser responsabilizado objetivamente pelo dano, a menos que comprove culpa exclusiva de terceiro ou da própria vítima. Esse marco legal ainda está em construção, o que cria incertezas sobre a extensão do dever de reparação e, portanto, sobre o controle efetivo do mercado sobre os outputs algorítmicos.

Finalmente, há limites técnicos na supervisão humana dos sistemas. Muitas inteligências artificiais modernas são intrinsecamente "*opacas*" – isto é, empregam milhões de parâmetros em redes neurais de difícil interpretação.

Como alertado por PASQUALE, 2015, p. 3-4 e p. 10-11, nessa "*sociedade da caixa-preta*", as próprias corporações ficam além do alcance do consumidor,

deslocando o poder informacional a corpos anônimos. Mesmo especialistas têm dificuldade em entender como decisões complexas são tomadas por IA.

Como consequência, o próprio controle humano sobre o ciclo de decisão torna-se parcial: humanos podem definir objetivos e limites iniciais, mas não acompanham passo a passo cada escolha feita pelo algoritmo. Esse fenômeno ressalta a necessidade de mecanismos complementares – como auditorias independentes ou testes de veracidade – para compensar os limites práticos da supervisão humana.

Nesse sentido, as leis de proteção de dados (Marco Civil da Internet e LGPD) já apontam caminhos ao exigir consentimento informado, transparência, segurança e prestação de contas no tratamento de dados. Esses princípios legais estabelecem que, mesmo em face da automação, permanece assegurado o controle mínimo do indivíduo sobre seu espaço informacional.

Em suma, embora a automação inove as relações de consumo, ela impõe riscoo, como privacidade, discriminação, incerteza que só serão controlados por meio de normas rigorosas e de mecanismos que ampliem a inteligibilidade dos sistemas além de esforços puramente técnicos.

4 PRIVACIDADE E A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

O bojo dos dados pessoais como ativo na economia digital pode ser considerado como elemento intrínseco às interações sociais, que leva ao Direito o desafio de readequar seus institutos para a tutela de um dos direitos mais sensíveis da personalidade: a privacidade.

Em uma sociedade caracterizada pela globalização e pela coleta massiva e contínua de informações, a proteção de dados transcende a noção tradicional de intimidade para se firmar como uma condição de autonomia individual, de livre desenvolvimento da personalidade e do exercício da cidadania. A capacidade de processamento algorítmico e a aplicação de IA em larga escala intensificam essa problemática, tornando necessária a construção de um regime jurídico eficaz.

Neste contexto, a Lei nº 13.709/2018, chamada de Lei Geral de Proteção de Dados Pessoais (LGPD), se consolida como o marco normativo fundamental no ordenamento brasileiro para a disciplina do tratamento de dados. Inspirada em paradigmas internacionais, a LGPD inaugura uma nova cultura de governança e responsabilidade, estabelecendo um arcabouço detalhado de princípios, direitos para os titulares e obrigações para os agentes de tratamento.

Sua vigência representa não apenas uma resposta legislativa, mas uma transição na forma como organizações públicas e privadas devem conceber suas operações e se relacionar com os indivíduos.

Este capítulo se dedica a explorar as múltiplas facetas deste novo diploma legal e seu impacto no cenário jurídico e tecnológico. A análise partirá dos fundamentos constitucionais que alicerçam o direito à proteção de dados como um direito fundamental autônomo.

Em seguida, adentrará na complexa relação entre a LGPD e o desenvolvimento de sistemas de Inteligência Artificial, analisando a inovação e a conformidade normativa. O estudo também se examinará sobre o consentimento do titular, e os desafios inerentes à sua obtenção e gestão em contextos de tratamento automatizado.

Por fim, observará como a lei reconfigura o instituto da responsabilidade civil e impõe novos deveres de segurança da informação, estabelecendo um regime próprio para a reparação de danos decorrentes de violações de dados pessoais.

4.1 Fundamentos constitucionais da proteção de dados pessoais

No ordenamento brasileiro, a proteção de dados pessoais tem por base princípios constitucionais já consolidados. A doutrina ressalta que a tutela da privacidade e da informação confere "*um novo e atual sentido à proteção da pessoa humana e da dignidade, da autonomia e das esferas de liberdade que lhes são inerentes*" (SARLET, 2021, p. 58-59). Em especial, entende-se que o tratamento de dados pessoais está estreitamente vinculado a cláusulas gerais como a dignidade da pessoa humana e o livre desenvolvimento da personalidade, bem como a direitos especiais de personalidade em privacidade e intimidade previstos no art. 5º, X e XI, da CFRB/88.

Nessa linha, (SARLET, 2020, p. 45) destaca que mesmo sem previsão expressa de um direito autônomo à proteção de dados na Carta de 1988, a CFRB/88 consagra implicitamente tal direito ao ser interpretada de forma harmônica: "*pode (e mesmo deve!) ser associado e reconduzido a alguns princípios e direitos fundamentais de caráter geral e especial, como o princípio da dignidade da pessoa humana, o direito fundamental (implicitamente positivado) ao livre desenvolvimento da personalidade … e dos direitos especiais de personalidade… os direitos à privacidade e à intimidade*".

Assim, tem-se que o fundamento constitucional direto mais próximo do direito à proteção de dados reside no direito ao livre desenvolvimento da personalidade – radicado na dignidade e na liberdade – o qual abrange o direito à livre disposição sobre os dados pessoais, denominado de autodeterminação informativa. Ou seja, o titular dos dados detém prerrogativa de decidir sobre a divulgação e utilização de suas informações pessoais, dentro dos limites do interesse geral (SARLET; SAAVEDRA, 2020, p. 33–49).

Embora a Constituição preveja, no art. 5º, inciso XII, o sigilo das comunicações de dados, essa proteção restringe-se à comunicação de dados (e não aos dados armazenados em si). A tutela de dados, então, via CFRB/88 ocorre de forma indireta,

especialmente por meio do *habeas data* (art. 5º, LXXII), ação constitucional que assegura ao indivíduo conhecer e retificar dados pessoais sob poder de entidades públicas. Na visão de (SARLET, 2020, p. 61), o *habeas data* deve ser visto como uma garantia procedimental do exercício da autodeterminação informacional.

No campo jurisprudencial, apesar de ainda não haver dispositivo constitucional expresso, o Supremo Tribunal Federal reconheceu que há um direito fundamental implícito de proteção de dados pessoais. Em renomado julgado, o STF assentou que esse direito autônomo é "implicitamente positivado" em nossa CFRB.

Essa compreensão ganhou concretude em 2020, quando o Tribunal analisou litígios envolvendo tratamento de dados sensíveis. Em casos emblemáticos – como a ADPF 695 (compartilhamento de dados entre órgãos de inteligência), e, principalmente, a ADI 6529/DF (Caso Sisbin) – a Corte delimitou o acesso a informações pessoais: no caso Sisbin, por exemplo, decidiu que os órgãos de inteligência só poderiam fornecer dados à ABIN mediante "*comprovado interesse público*", vedando qualquer uso para fins particulares.

Esses precedentes ilustram a aplicação concreta do direito à proteção de dados no contexto brasileiro: como expõe Molinaro e Sarlet, a proteção de dados pessoais e o respectivo direito fundamental "confere um novo e atual sentido à proteção da pessoa humana e da dignidade, da autonomia e das esferas de liberdade que lhes são inerentes", reafirmando a convergência entre dignidade, autodeterminação informativa e privacidade.

Recentemente, a Emenda Constitucional nº 115/2022 elevou esse entendimento a texto constitucional. Com a reforma, foi acrescentado ao art. 5º, inciso LXXIX, o dispositivo que assegura expressamente "o direito à proteção dos dados pessoais, inclusive nos meios digitais". Erm outras palavras, a proteção de dados passa a figurar claramente no rol de direitos fundamentais da CRFB/88.

Essa inclusão constitucional reforça a importância de uma regulação robusta e da fiscalização pela Autoridade Nacional de Proteção de Dados (ANPD), sinalizando que a LGPD deve ser interpretada em harmonia com essa nova base constitucional. Em suma, no plano constitucional a proteção de dados pessoais emerge como direito

inserido no núcleo da dignidade e liberdade da pessoa, refletindo-se em novas exigências normativas e no fortalecimento de instituições de fiscalização e controle.

4.2 A LGPD e seus impactos no desenvolvimento e uso de IA

A Lei Geral de Proteção de Dados (Lei nº 13.709/2018) ocupa posição central na regulação do uso de tecnologias de IA que envolvam tratamento de dados pessoais. Embora a LGPD não tenha nascido com foco exclusivo em inteligência artificial, seus dispositivos normativos fundamentais servem de balizas legais para qualquer manipulação automatizada de informações pessoais.

O art. 1º da LGPD estabelece, como objetivo da lei, “proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural”.

Já o art. 2º enumera expressamente como fundamentos da proteção de dados “o *respeito à privacidade”* e “*a autodeterminação informativa”*, além da liberdade de expressão, inovação tecnológica, entre outros. Esses preceitos vinculam diretamente a aplicação de IA a valores constitucionais: qualquer modelo ou algoritmo que trate dados deve observar a privacidade e a autonomia do titular, prevendo mecanismos de consentimento, transparência e propósito legítimo. Outrossim, a LGPD consolida em lei o compromisso constitucional com a privacidade, definindo diretrizes que impactam o desenvolvimento de sistemas inteligentes.

No contexto da IA, a LGPD passou a ser vista como o início da regulação do setor no Brasil. Em particular, o art. 20 da lei assegura ao titular dos dados o “direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses”. Na visão de NARDI, 2023, p. 1.742 essa previsão consagra a obrigação de explicabilidade em processos decisórios automatizados e marca o primeiro instrumento legal nacional a enfrentar, ainda que de forma incipiente, o fenômeno da IA.

A importância dessa norma se torna evidente quando se consideram aplicações típicas de IA – como análise de crédito, triagem de currículos ou diagnósticos médicos

automatizados – que podem impactar direitos dos indivíduos. Todavia, observa-se que o art. 20 tem alcance restrito, só se aplica a decisões inteiramente automatizadas.

Na prática, muitos sistemas de IA atuais operam sob supervisão humana parcial (processos híbridos), casos em que o direito à explicação não é garantido pela LGPD. Esse hiato tem sido apontado como desafio regulatório: como destaca SILVA; GUIMARÃES, 2023, p. 725–726, a regra do art. 20 da LGPD restringe sua aplicação a decisões tomadas inteiramente pelas chamadas ferramentas inteligentes, deixando de fora situações de decisão mista. Em complemento, embora a LGPD preveja que o controlador deve auditar medidas recusadas de transparência à ANPD, ainda há dúvidas sobre a efetiva intervenção da autoridade e sobre como assegurar o direito à explicação em larga escala (SILVA; GUIMARÃES, 2023, p. 728).

No terreno econômico e tecnológico, a IA tem desempenhado papel estratégico no Brasil. Iniciativas governamentais indicam um estímulo à inovação: em 2017 foi criada a Associação Brasileira de Inteligência Artificial (ABRIA), que fomenta parcerias público-privadas, intercâmbio de dados abertos e projetos de pesquisa em IA como prioridade estratégica.

Esse movimento confere à IA relevante papel no desenvolvimento nacional. O uso de IA pelas empresas tornou-se assemelhado à um selo de qualidade – associado à soberania e à competitividade internacional dos países – otimização da balança comercial e atração de investimentos externos. Ou seja, por um lado a inteligência artificial é vista como vetor de crescimento econômico e de inovação tecnológica – indústria 4.0, comércio eletrônico, serviços inteligentes etc. –, motivando empresas e governos a incorporá-la.

Por outro lado, tal dependência crescente de IA impõe tensão entre o estímulo à inovação e a proteção efetiva de direitos individuais. Conforme salientado nos trabalhos recentes, a adoção desregulada de sistemas inteligentes pode colocar em risco liberdades fundamentais. Casos como a divulgação imprudente de dados por assistentes virtuais e o escândalo *Cambridge Analytica* evidenciaram como o uso massivo de IA em grandes bases de dados — muitas vezes sem filtros adequados — acarreta graves riscos à privacidade e à autodeterminação informativa.

Diante dessa dicotomia, surgem desafios regulatórios complexos. Embora LGPD e leis correlatas. como o Marco Civil da Internet representem avanços, persistem lacunas em face do ritmo acelerado da IA. Em especial, percebe-se a necessidade de reforçar a governança algorítmica e a atuação da Autoridade Nacional de Proteção de Dados (ANPD).

Ao reforçar a importância do marco regulatório, destaca-se que a Emenda Constitucional 115/2022 "*reforça a importância de uma regulação robusta e da fiscalização pela ANPD*", indicando o papel central dessa autarquia em disciplinar novas técnicas. Conforme concluem estudos atuais, medidas como exigência de transparência algorítmica, responsabilização objetiva por danos causados por IA e a revisão judicial de decisões automatizadas são ferramentas essenciais para ampliar a efetividade da LGPD no contexto da IA (NARDI, 2023, p. 1812–1820).

Tais instrumentos visam criar um equilíbrio dinâmico entre inovação e proteção: por um lado, incentivam empresas a adotar padrões éticos e seguros; por outro, garantem que o avanço tecnológico não subjugue direitos fundamentais.

Em suma, a LGPD estabelece bases legais importantes para o uso da IA, mas o desafio regulatório consiste em aperfeiçoar essas regras e fiscalizações para que a inovação seja desenvolvida em sintonia com o respeito à privacidade, à dignidade e à autonomia dos titulares de dados.

4.3 O consentimento do titular e os desafios do tratamento automatizado de dados

Na LGPD, o consentimento é disciplinado como uma das bases legais para o tratamento de dados pessoais (art. 7º, I). Constitui-se em "manifestação de vontade livre, informada e inequívoca" pela qual o titular concorda com o tratamento de seus dados para finalidade específica. Em outras palavras, exige-se que o consentimento seja claro, expresso e sem vícios, de forma que o titular compreenda plenamente as consequências de sua decisão. Prevê-se, inclusive, o direito de revogação do consentimento a qualquer tempo, de forma gratuita e facilitada (art. 8º, §5º), assim que manifestada pelo titular (com efeito *ex nunc*).

Em caso de revogação, o controlador deve informar o titular sobre a viabilidade de continuidade do tratamento em outras bases legais, conforme previsto no art. 18, por exemplo, hipóteses de arquivamento legal. Ademais, a lei determina que dados pessoalmente coletados com base no consentimento sejam eliminados quando cessada sua finalidade e revogado o consentimento (art. 18, VI).

A função do consentimento vai além de autorizar o tratamento; trata-se também de instrumento de transparência e responsabilização, conforme destacam autores como PINHEIRO, 2021, p. 133. Em ambiente digital, a sensibilidade da informação pessoal faz do consentimento sobre a questão fundamental para concretizar o direito do usuário de conhecer a finalidade da coleta e de acessar seu conteúdo, garantindo assim a liberdade e a privacidade.

Para PINHEIRO, 2021, p. 133, constitui "*garantia da legalidade do tratamento de dados que foi ou será realizado*". No entanto, críticos como Bruno Ricaardo Bioni aponta os limites do modelo centrado no consentimento. Em seu texto alerta que é inadequado tratar a proteção de dados apenas como extensão do direito à privacidade, considerando-o, antes, um direito autônomo que exige mecanismos próprios de tutela. Essa perspectiva sugere que a simples formalização do consentimento não basta: o poder informacional das empresas e a assimetria de poder no ambiente on-line podem transformar o consentimento em mero ato formal, sem efetiva autodeterminação do titular.

O tratamento automatizado de dados, em especial pelas tecnologias de *Big Data* e Inteligência Artificial, agrava esses desafios. A coleta massiva de informações pessoais e o uso de algoritmos preditivos podem comprometer o caráter livre e informado do consentimento. Por exemplo, é praticamente impossível que o usuário preveja de antemão todos os usos futuros de seus dados em sistemas de IA ou que compreenda plenamente os critérios automáticos de perfilamento. Nesse contexto, a LGPD prevê dispositivos específicos.

O art. 20 assegura ao titular "direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais" que afetem seus interesses. Esse direito aplica-se a decisões de crédito, perfil de consumo ou

aspectos da personalidade definidos por algoritmos, garantindo a possibilidade de revisão humana das decisões automatizadas.

Complementarmente, o parágrafo 1º do mesmo artigo impõe ao controlador o dever de fornecer, quando solicitado, informações claras sobre os critérios e procedimentos utilizados na decisão automatizada. Essas medidas buscam conter efeitos discriminatórios ou arbitrários da automação, ainda que a LGPD não proíba o uso de IA em si mesma.

No entanto, diferentemente da GDPR europeia (art. 22), a LGPD não estabelece um veto geral ao processamento automatizado, limitando-se a direitos de explicação e revisão. O consentimento continua sendo base legal autorizadora (art. 7º, I) para diversas operações, mas sua eficácia requer mecanismos complementares de proteção.

A exigência de transparência, o princípio da minimização dos dados coletados e obrigações de segurança por design (*privacy by design*) visam equilibrar a necessidade de inovações tecnológicas com a salvaguarda dos direitos dos titulares.

Em última instância, como observa a doutrina, o tratamento de dados no contexto de *Big Data* cria novos desafios para a autodeterminação informacional: exige-se interpretação sistemática da LGPD, analisando princípios como finalidade, necessidade e segurança, além de possível apoio em normas do Código de Defesa do Consumidor. Por exemplo, o CDC exige consentimento prévio para cadastros de consumidores (art. 43), reforçando a ideia de que qualquer tratamento automatizado em relações de consumo deva observar ainda mais rigor na obtenção do consentimento. De modo geral, a que o modelo de consentimento da LGPD, embora fundamental, demanda análise crítica e acompanhamento técnico constante para não se tornar ineficaz diante das práticas massivas de processamento automatizado.

4.4 Responsabilidade civil e segurança da informação na perspectiva da LGPD

O Capítulo VI da LGPD institui um regime abrangente de responsabilidade civil e de segurança da informação. O artigo 46 impõe aos agentes de tratamento (controlador e operador) a obrigação de adotar medidas técnicas e administrativas de

segurança aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração ou qualquer forma de tratamento inadequado.

Em complemento, o art. 50 prevê que tais medidas devem ser proporcionais ao risco do tratamento, considerando especialmente sua gravidade. Esses dispositivos refletem o princípio da prevenção e o enfoque de *privacy by design*, exigindo que as empresas avaliem riscos e implantem controles eficientes para mitigar incidentes. Em caso de incidente grave, o controlador deve comunicar o fato à Autoridade Nacional de Proteção de Dados e ao titular afetado (art. 48), sob pena de sanções administrativas (art. 52).

A consequência central da violação de deveres de segurança está no art. 42 da LGPD, que prevê a indenização por danos materiais, morais e coletivos decorrentes de tratamento irregular de dados. Controladores e operadores são obrigados a reparar dano patrimonial, moral, individual ou coletivo causado a terceiro em razão de atividade de tratamento de dados em violação à legislação de proteção de dados.

Note-se que a reparação depende do requisito triplo: (i) exercício de atividade de tratamento, (ii) ocorrência de dano e (iii) inobservância da lei (violação da LGPD). Não basta o mero dano decorrente do uso de dados; é imprescindível demonstrar que a conduta do agente contrariou os mandamentos legais. Esse princípio condicionalista é reforçado pelos art. 43 e 44 da LGPD.

O art. 43 estabelece hipóteses excludentes de responsabilidade – por exemplo, prova de observância da lei ou de ordem legal – definindo que “só não serão responsabilizados quando provarem […] que não houve violação à legislação de proteção de dados”. Por sua vez, o art. 44, caput dispõe que o tratamento só é irregular se descumprir a LGPD ou não fornecer a segurança que o titular pode esperar; inversamente, observando-se a lei e garantindo-se a segurança devida, o tratamento não será considerado irregular. Em síntese, a responsabilidade civil na LGPD pressupõe culpa: é necessária a violação de um dever para ensejar indenização. Como observa (TASSO, 2020, p. 139-140) “é cediço que todo o sistema de responsabilidade civil na LGPD [está] intrinsecamente vinculado ao elemento culpa”.

Em contrapartida, parte da doutrina advoga pela aplicação objetiva da responsabilidade, considerando a atividade de tratamento de dados como de risco inerente. Argumenta-se que, dado o potencial gravíssimo de lesão aos direitos fundamentais do titular, deveria haver presunção de culpa nas operações de alto risco (MENDES; DONEDA, 2018, p. 137. Entretanto, a letra da lei reflete entendimento diverso: não menciona a expressão “independentemente de culpa” (como faz o CDC e o antigo art. 927 do CC), e, conforme Tasso, isso “sugere preferência por regime de responsabilidade subjetiva”. Na visão de Tasso, interpretar a LGPD como objetiva anularia os deveres específicos de segurança, pois “redundaria na conclusão de que de nada adiantaria o cumprimento dos deveres se, qualquer que fosse o incidente, a responsabilidade pela reparação estivesse configurada”.

Quanto à interface com o Código Civil, observa-se coerência: o CC estabelece, como regra geral (art. 927), a reparação do dano por ato ilícito, admitindo culpa presumida apenas em casos específicos (art. 936, 927, §1º pós-Código). Assim, a LGPD não cria um regime radicalmente diverso, alinhando-se à visão de que a responsabilidade civil demanda análise de culpa (dolo ou culpa) do agente. Por outro lado, no âmbito do Código de Defesa do Consumidor (CDC), o conflito é mais complexo. A LGPD positivou em seu art. 45 que as normas de proteção de dados aplicam-se às relações de consumo, vinculando os microssistemas. Em tese, se a violação de dados pessoais ocorrer em relação de consumo, deve ser considerado o regime objetivo do CDC (arts. 12 e 14). Nesse sentido, Tasso conclui que “o tratamento jurídico da responsabilidade objetiva previsto no microssistema do Código de Defesa do Consumidor” deve prevalecer quando há conexão com relação de consumo. Em outras palavras, a LGPD adota regra geral subjetiva, mas quando o dado pessoal é utilizado em contexto de produto/serviço, convém aplicar o ônus objetivo do CDC em favor do consumidor, dado o caráter fundamental dessa proteção.

Contudo, mesmo admitindo a responsabilidade objetiva no campo consumerista, as excludentes de responsabilidade da LGPD (art. 43) devem ser observadas. Em comparação, o CDC prevê como hipótese de exclusão a não colocação do produto no mercado (art. 12, §3º, II), o que equivale a “objeto binário” (o produto não existir ou existir). Já a LGPD exige um dever adicional: o controlador que comprovar ter adotado diligência adequada – notadamente as medidas de segurança técnicas e

administrativas – estará exon erado. Em suma, nos termos da LGPD, só responderá quem demonstrar descumprir a lei de proteção de dados; do contrário, havendo boa-fé e cumprimento dos deveres, não há dano ilícito a ser reparado.

É nesse cenário que a segurança da informação assume papel central. A violação sistemática dos deveres de prevenção e segurança transforma-se em conduto ilícita. Se o controlador não implementar as salvaguardas previstas no art. 46 e seus correlatos, responde pelos danos decorrentes desse “incidente de segurança”. Por outro lado, o mero sinistro não implica culpa objetiva: se forem observadas todas as normas e padrões de segurança adequados, não se fala em tratamento irregular nem em obrigação de indenizar. Segundo Tasso, a LGPD “fixou um padrão de conduta” e “cobra o cumprimento desses deveres”, modulando a reparação ao contexto fático e técnico. Tal sistema busca atender ao princípio da prevenção e da responsabilização pelo risco informacional, sem, porém, inibir indevidamente o fluxo econômico de dados previsto nos fundamentos da lei.

Em conclusão, a LGPD instituiu uma rede de regras de segurança e responsabilidade civil que dialoga com o CDC e o CC. Como (TASSO, 2020, p. 25-140), a lei criou “*u*m sistema de responsabilidade civil compatível com o Código Civil e o Código de Defesa do Consumidor”, elegendo por regra a responsabilização subjetiva em consonância com o CC e, nas relações consumeristas, permitindo a aplicação objetiva do CDC.

Assim, a responsabilização recai sobre aquele que violar os padrões de proteção e segurança da informação, impondo-lhe o dever de indenizar, enquanto incentiva o cumprimento diligente de normas e boas práticas de governança de dados.

5 RESPONSABILIZAÇÃO POR DADOS FRAUDULENTOS E INFORMAÇÕES EQUÍVOCAS

A crescente autonomia dos sistemas de IA e a sua integração como intermediários nas relações de consumo e prestação de serviços trazem consigo um risco inerente e de elevada complexidade: a disseminação de informações equívocas, imprecisas ou deliberadamente fraudulentas.

Quando um output informacional gerado por um algoritmo causa prejuízo a um indivíduo, surge a questão a quem incumbe o dever de reparar. A presença de humanos em cadeias de programação, treinamento de dados e operação de sistemas automatizados torna a atribuição de responsabilidade civil uma tarefa intrincada, que desafia o Direito.

A falha informacional no ambiente digital transcende o mero equívoco, podendo configurar-se como um defeito do serviço ou do produto, na medida em que a informação correta constitui o resultado esperado pelo usuário. A confiança depositada em assistentes digitais e chatbots como fontes fidedignas de dados agrava o potencial lesivo, necessitando respostas pelo ordenamento jurídico para que sejam, ao mesmo tempo, protetivas para a parte vulnerável e capazes de incentivar boas práticas de governança e segurança por parte dos desenvolvedores e fornecedores de tecnologia. A responsabilidade, neste contexto, não apenas cumpre sua função reparatória, mas também assume um caráter preventivo e pedagógico.

Este capítulo se aprofundará na análise dos mecanismos de responsabilização civil decorrentes da veiculação de dados falhos por sistemas automatizados com o exame do conceito de erro informacional e de seus impactos específicos no Direito do Consumidor.

Por conseguinte, se concentrará na imputação de responsabilidade por falhas sistêmicas em chatbots e assistentes digitais, investigando os critérios para a identificação do nexo de causalidade entre o defeito tecnológico e o dano.

Por fim, para consolidar a investigação será promovida uma análise da jurisprudência nacional e estrangeira, identificando as tendências e os fundamentos que vêm sendo adotados pelos tribunais para solucionar estes litígios.

5.1 Erro informacional e seus impactos no direito do consumidor

O fenômeno do erro informacional no contexto da inteligência artificial refere-se à circulação de dados incorretos ou enganosos e à falta de clareza nas informações fornecidas aos consumidores. Essa problemática aprofunda a já existente assimetria informacional nas relações de consumo digitais, agravando a vulnerabilidade do consumidor.

Estudos recentes apontam que a expansão de sistemas de IA no mercado tem intensificado a desigualdade de informações entre fornecedores e consumidores, muitas vezes em prejuízo da autonomia destes últimos. Conforme destaca VELLOSO, 2025, p. 87-95 “os resultados evidenciam que a assimetria informacional se agrava, comprometendo a autonomia e a autodeterminação dos indivíduos, além de favorecer práticas comerciais abusivas”. Ou seja, quando o consumidor não dispõe de informações claras e precisas – ou recebe informações equívocas – sua capacidade de escolha livre e consciente é afetada, podendo ser direcionada por interesses do fornecedor.

A vulnerabilidade do consumidor frente a sistemas de IA também se manifesta pela opacidade algorítmica e falta de transparência dessas tecnologias. Muitas vezes, o consumidor nem sequer percebe que está sendo alvo de tratamento massivo de dados e decisões automatizadas em suas interações de consumo. LUNARDI, 2022, p. 75-83 observa que, na sociedade de consumo digital, o indivíduo passa a ficar exposto a uma série de riscos tecnológicos, sendo “*bombardeado por sugestões e padrões de consumo que poderão surtir reflexos devastadores na sua liberdade de escolha*”. Esse bombardeio informacional fornecido por algoritmos pode induzir o consumidor a erros de julgamento ou escolhas contra seus interesses, especialmente quando há perfilização oculta ou recomendação manipulativa de produtos/serviços.

Ademais, a falta de transparência sobre como funcionam esses algoritmos torna difícil para o consumidor discernir se as informações são neutras ou enviesadas. MARQUES, 2014, p. 137-139 denomina de iniquidade de transparência o fato de que, no ambiente da IA, “*as relações de consumo estão cada vez mais regadas de iniquidade de transparência... tanto é assim que se tornou lugar-comum referir-se ao*

funcionamento de tais tecnologias sob a denominação de black boxes, em alusão ao fato de que esses sistemas inteligentes internalizam dados e dão feedbacks de maneiras não facilmente auditáveis ou compreensíveis para seres humanos".

Em outras palavras, para o consumidor o processo decisório dos algoritmos não sabe quais dados foram usados nem quais critérios levaram àquela informação ou recomendação apresentada, o que aprofunda sua vulnerabilidade.

Do ponto de vista jurídico, o direito à informação é um pilar fundamental do direito do consumidor, funcionando como contrapeso à vulnerabilidade informacional. O Código de Defesa do Consumidor (CDC) consagra, em seu art. 6º, III, o direito básico do consumidor à informação adequada e clara sobre produtos e serviços, incluindo suas características, composição, qualidade, preço e riscos.

Trata-se de garantir transparência e compreensão para que o consumidor exerça sua autonomia de forma consciente. BARROS, 2024, p. 259-267 relembra que esse dispositivo assegura ao consumidor "*o direito de receber informações precisas e adequadas sobre os produtos e serviços que estão adquirindo, permitindo a tomada de decisões conscientes e seguras*".

Em complemento, o CDC reconhece no art. 4º, I, a vulnerabilidade do consumidor no mercado de consumo, impondo deveres de lealdade e transparência aos fornecedores.

Desse modo, a lei exige que as informações sejam claras, verídicas e disponibilizadas em todas as fases da relação de consumo, desde a publicidade e oferta (fase pré-contratual), passando pela contratação, até o pós-venda. Qualquer falha informacional – seja pela omissão de dados importantes, seja pela veiculação de conteúdo falso ou impreciso – fere diretamente o direito à informação e pode configurar prática abusiva.

No contexto de sistemas de IA, essas obrigações ganham novos contornos. Há uma demanda crescente por transparência algorítmica, isto é, pelo dever do fornecedor informar ao usuário que determinado serviço é prestado por meio de algoritmos e quais são, dentro do possível, os critérios utilizados por essas ferramentas inteligentes.

A LGPD (Lei Geral de Proteção de Dados Pessoais) reforça tal necessidade ao estabelecer, como princípio, a transparência no tratamento de dados (art. 6º, VI, LGPD), o que converge com o direito informacional do consumidor. Em última análise, erro informacional oriundo de IA – como dados fraudulentos inseridos num sistema ou respostas equívocas geradas por um *chatbot* – pode induzir o consumidor em erro, maculando seu consentimento ou levando-o a decisões lesivas.

Nesses casos, aplicam-se os mecanismos protetivos do CDC, inclusive com possibilidade de responsabilização do fornecedor pelos danos causados. A própria integração de IA nas relações de consumo exige reinterpretações do dever de informar, para abarcar não apenas informações tradicionais sobre produtos, mas também esclarecimentos sobre o uso de algoritmos na oferta ou prestação de serviços.

Somente com informação clara, acessível e completa o consumidor poderá exercer plenamente sua liberdade de escolha, mesmo em um ambiente permeado por inteligência artificial.

5.2 A responsabilidade civil por falhas sistêmicas em *chatbots* e assistentes digitais

A incorporação de *chatbots* e assistentes digitais nos serviços ao consumidor traz à tona a complexa questão da responsabilidade civil por falhas sistêmicas dessas inteligências artificiais. Tais falhas sistêmicas podem se manifestar, por exemplo, quando um chatbot fornece informações equívocas de forma recorrente ou quando um assistente virtual incorre em erros devido a bugs algorítmicos ou dados de treinamento enviesados.

Um caso emblemático foi o da chatbotTay, da Microsoft, que em poucas horas interagindo com usuários passou a produzir mensagens ofensivas e discriminatórias, levantando o questionamento: quem responde por um “*erro inumano*” cometido por uma IA autônoma – o desenvolvedor, o proprietário da plataforma ou a própria máquina?

Situações assim ilustram o desafio de atribuir culpa ou negligência em sistemas dotados de certa autonomia decisória e opacidade algorítmica. De fato, tal vulnerabilidade do usuário é agravada quando a opacidade da IA inviabiliza a transparência no processo de tomadas de decisões, o que dificulta identificar a origem exata da falha e, consequentemente, quem foi o agente responsável.

Diante dessa dificuldade de individuar a culpa em falhas de sistemas de IA, a doutrina e a legislação buscam caminhos para garantir a devida responsabilização e a proteção do consumidor. Uma abordagem recorrente é recorrer à responsabilidade objetiva, fundamentada na teoria do risco.

Em essência, entende-se que quem se beneficia e introduz a tecnologia deve arcar com os riscos que ela gera, independentemente de culpa. Essa visão ganha força especialmente em casos de falha sistêmica onde não há um ato culposo humano claro, mas sim um mau funcionamento inerente ao sistema autônomo.

FARIA, 2022, p. 285-293 destaca que, no contexto europeu, optou-se por adotar a responsabilidade objetiva para sistemas de IA de alto risco exatamente por ter se "*mostrado necessária diante da dificuldade, ou até mesmo impossibilidade, de se comprovar a culpa dos agentes responsáveis pelos danos causados pela inteligência artificial, evitando-se assim uma inaceitável impunidade"*. Em outras palavras, exigir prova de culpa humana em acidentes causados por IA altamente autônomas poderia levar à não reparação das vítimas – uma injustiça que o ordenamento não pode tolerar.

Assim, propõe-se imputar automaticamente a responsabilidade ao operador ou fornecedor da tecnologia, cabendo a este depois eventualmente buscar o ressarcimento de terceiros se couber.

No Brasil, apesar de não haver lei específica sobre IA, o ordenamento já dispõe de ferramentas para enfrentar essas situações, notadamente através do sistema dual de responsabilidade civil (objetiva e subjetiva) e da incidência do Código de Defesa do Consumidor.

De acordo com FARIA, 2022, p. 285-293, o modelo brasileiro permite conciliar a resposta jurídica aos danos de IA adotando "*a responsabilidade objetiva pelo risco da*

atividade àqueles [casos] que ofereçam grau de risco e de autonomia mais elevado e a subjetiva nos demais casos". Ou seja, para *chatbots* e assistentes digitais cuja operação apresenta riscos significativos ao consumidor – por exemplo, por poderem causar danos patrimoniais ou morais em larga escala devido a erros sistêmicos – aplicar-se-ia a responsabilidade objetiva (dispensando a prova de culpa do fornecedor).

Nos casos de menor risco ou em que a IA atua apenas como ferramenta auxiliar sob alto grau de supervisão humana, poderia ainda caber a responsabilidade subjetiva (com culpa presumida, na forma do art. 14, §3º do CDC, por exemplo). Essa calibração conforme o nível de risco evita tanto a impunidade em casos graves quanto a sobrecarga injustificada em casos triviais.

Importante notar que, no âmbito das relações de consumo, *chatbots* e IAs prestadoras de serviço equiparam-se a fornecedores para fins de responsabilidade. Se um assistente digital presta um serviço defeituoso ou inseguro, incide o art. 14 do CDC (fato do serviço), responsabilizando objetivamente toda a cadeia de fornecedores envolvida. Aliás, a doutrina já vem ampliando o conceito de fornecedor para abarcar os agentes técnicos por trás da IA. Os desenvolvedores de software ou algoritmos inseridos no mercado de consumo devem ser considerados parte da cadeia produtiva, de modo a imputar-lhes o dever de reparação em caso de danos decorrentes do sistema de inteligência artificial, com base nos arts. 12 e 14 do CDC.

Desse modo, se um *chatbot* bancário causar um prejuízo ao fornecer um conselho financeiro desastroso, tanto a instituição fornecedora do serviço quanto eventualmente a empresa desenvolvedora do algoritmo poderão ser chamadas a indenizar o consumidor lesado, pois todos integram a atividade de risco que gerou o dano.

A caracterização da falha sistêmica de uma IA como defeito do produto ou do serviço é tema sensível. Em certos casos, a IA pode ter um comportamento inesperado sem que haja um defeito de programação aparente – é o chamado viés emergente da aprendizagem de máquina. Contudo, mesmo nesses cenários, prevalece o entendimento de que se trata de um risco inerente à tecnologia, que não deve exonerar o fornecedor.

Nas palavras de BARBOSA, 2019, p. 215-223, os danos causados pelo robô inteligente podem derivar de sua atuação autônoma, a qual "*longe de ser uma marca de defeituosidade, se traduz numa característica intrínseca*" do sistema. Ainda assim, na hipótese de comportamento extraordinário ou não previamente advertido ao consumidor, é razoável considerar que o fornecedor permanece responsável pelo evento danoso.

Como sintetiza FARIA, 2022, p. 285-293, a responsabilidade do fornecedor "*vai além da constatação do ordinário defeito, para abranger situações de extraordinariedade na atividade comercializada, com fulcro na teoria do risco, (...) por força do risco inerente ao funcionamento do sistema. Trata-se de fortuito interno que, diferentemente do fortuito externo, não afasta a responsabilidade do fornecedor*".

Em termos práticos, isso significa que mesmo um erro inesperado de um assistente digital – ainda que decorrente de sua autonomia e não de uma falha de fabricação identificável – será tratado como risco do empreendimento (um fortuito interno da atividade de IA), não eximindo o dever de indenizar. Tal posição impede que os fornecedores escapem da responsabilização alegando que o erro foi imprevisível, já que a imprevisibilidade, nesse caso, faz parte do risco da tecnologia que eles introduziram no mercado.

Além de reparar os danos causados, a responsabilização civil por falhas sistêmicas em IA desempenha também uma crucial função preventiva e regulatória. A perspectiva tradicional da responsabilidade civil evoluiu para não apenas compensar a vítima, mas também estimular padrões mais seguros de conduta por parte dos fornecedores. SILVA, 2021, p. 279-287 enfatiza que a função preventiva ganha destaque no contexto de inovações tecnológicas, pois "*assume caráter de extrema relevância no referido contexto de riscos, pois visa assegurar padrões de segurança, evitando a ocorrência de danos*".

Ao sujeitar fabricantes e desenvolvedores de *chatbots* a uma responsabilidade objetiva por falhas de seus sistemas, o ordenamento incentiva que tais agentes invistam em melhorias de segurança, testes rigorosos e mecanismos de controle dos algoritmos antes de lançá-los no mercado.

Trata-se de aplicar, aqui, a máxima de que é melhor prevenir do que remediar: a possibilidade de ter que indenizar pesadamente os consumidores lesados por uma decisão errônea de uma IA estimula as empresas a adotarem uma postura diligente e proativa, mitigando riscos (princípio da prevenção). Em complemento, a responsabilização também tem um efeito pedagógico e dissuasório (teoria do desestímulo), desmotivando comportamentos negligentes ou aventureiros no desenvolvimento de IA de uso massivo.

Por fim, vale mencionar que a própria comunidade internacional caminha no sentido de combinar *accountability* tecnológica com proteção do consumidor. Iniciativas legislativas na Europa discutem seguros obrigatórios para operadores de IA de alto risco e fundos de compensação, aliados a esquemas de responsabilidade objetiva, justamente para garantir que sempre haja um responsável solvente para arcar com prejuízos causados por falhas algorítmicas.

No Brasil, embora ainda sem lei específica, os fundamentos do CDC e do Código Civil mostram-se flexíveis o suficiente para, mediante interpretação sistemática e diálogo de fontes, acomodar os novos desafios impostos pelos *chatbots* e assistentes digitais.

Falhas sistêmicas em IA não são terra sem lei: ao contrário, sujeitam-se às teorias clássicas de defeito do produto/serviço e risco do empreendimento, adaptadas ao cenário tecnológico atual, sempre visando a proteção do consumidor vulnerável e a prevenção de novos danos. A mensagem que se extrai é clara – a alta tecnologia não é sinônimo de irresponsabilidade, devendo prevalecer o princípio da confiança e segurança nas relações de consumo, mesmo mediadas por inteligências artificiais.

5.3 Prejuízos patrimoniais e extrapatrimoniais decorrentes de desinformação

A disseminação de informações falsas ou dados fraudulentos – fenômeno comumente referido como desinformação – acarreta múltiplas formas de prejuízo jurídico, abrangendo danos de ordem patrimonial e extrapatrimonial. Em termos conceituais, dano patrimonial é aquele de natureza econômica, traduzido na

diminuição do patrimônio da vítima ou na frustração de uma vantagem financeira esperada.

Já o dano extrapatrimonial relaciona-se à lesão à dignidade humana em suas diversas expressões (honra, reputação, privacidade, integridade psíquica, etc.), atingindo direitos de personalidade protegidos pela ordem jurídica. Desse modo, enquanto a responsabilidade civil por dano patrimonial busca repararintegralmente o prejuízo econômico sofrido, a decorrente de dano extrapatrimonial tem por fim compensar a ofensa à esfera personalíssima da vítima.

No contexto da desinformação, os danos patrimoniais podem se manifestar de formas diretas ou indiretas. Por exemplo, a veiculação de uma notícia falsa sobre a solvência de uma empresa pode desencadear perdas financeiras aos investidores ou ao próprio negócio, configurando prejuízo material indenizável. Do mesmo modo, um consumidor induzido em erro por propaganda enganosa (espécie de desinformação comercial) pode realizar gastos desnecessários ou sofrer perdas econômicas concretas.

Nesses casos, havendo nexo causal entre a informação equivocada e a perda econômica, cabe a reparação civil do dano patrimonial, nos termos do art. 927 do Código Civil brasileiro. Cabe observar, no entanto, que em alguns ordenamentos estrangeiros discute-se a limitação da responsabilidade por danos exclusivamente econômicosquando não há violação a um direito absoluto: no Direito português, por exemplo, entende-se que os chamados “danos patrimoniais puros” em regra não são ressarcíveis em sede extracontratual, salvo quando resultantes da violação de norma protetiva específica ou de abuso de direito.

Essa perspectiva restritiva visa evitar a banalização de pedidos indenizatórios por meros aborrecimentos econômicos cotidianos, reservando a indenização patrimonial para prejuízos que ultrapassem os riscos normais da vida em sociedade.

Por sua vez, os danos extrapatrimoniais decorrentes de desinformação revelam especial gravidade, dada a natureza dos bens jurídicos atingidos. A honra objetiva e subjetiva, a imagem, a intimidade, a identidade pessoal e mesmo a boa reputação

social estão entre os direitos da personalidade potencialmente lesados por notícias falsas ou conteúdo enganoso.

Assim, uma fake news difamatória que atribui falsamente a alguém a prática de um crime ou conduta imoral viola seu direito à honra e à imagem, gerando o direito à indenização por dano moral.

Ademais, a manipulação de dados e informações por sistemas de inteligência artificial (IA) pode igualmente resultar em prejuízos de ordem patrimonial e moral aos indivíduos. As decisões algorítmicas equívocas ou algoritmos enviesados podem gerar consequências danosas aos usuários, atingindo tanto seu patrimônio quanto seus direitos imateriais. Por exemplo, a utilização de dados pessoais incorretos ou de critérios discriminatórios em um algoritmo de crédito pode levar à negação injusta de um empréstimo (dano material) e simultaneamente macular a reputação ou provocar abalo emocional no consumidor preterido (dano moral).

LUNARDI, 2021, p. 141 adverte que a coleta e uso de dados de forma não transparente e sem critérios éticos, quando inseridos em sistemas de IA, podem causar sérios danos aos consumidores, refletindo-se inclusive em discriminações de cunho racial, sexista ou religioso.

Tais práticas lesivas afrontam valores da dignidade da pessoa humana e evidenciam a necessidade de se reavaliar os esquemas de imputação de responsabilidade civil, de modo a assegurar a devida reparação dos danos causados e coibir violações a direitos fundamentais na sociedade da informação.

Importante salientar que os efeitos danosos da desinformação podem transcender a esfera individual, alcançando dimensão coletiva ou difusa. A propagação massiva de fake news pode abalar a confiança nas instituições, comprometer o debate público e até influenciar indevidamente processos democráticos (como eleições).

Nessa hipótese, embora haja inegável prejuízo social – por exemplo, o resultado distorcido de um pleito eleitoral em função de notícias falsas –, a configuração de um sujeito lesado direto nem sempre é evidente. Fala-se em lesados indiretos ou vítimas difusas: cidadãos que, embora não tenham um direito subjetivo individual violado de

forma imediata, sofrem os malefícios coletivos gerados pelo ecossistema de desinformação.

A dissertação de OLIVEIRA, 2022, p. 169-177 ressalta que essa coletivização do dano dificulta sobremaneira o recurso à responsabilidade civil tradicional, concebida para tutelar interesses individuais determinados. Além disso, para que um dano moral coletivo seja indenizável, há de se perquirir a gravidade da lesão e sua repercussão além dos dissabores comuns da vida em sociedade.

Em síntese, a desinformação sistêmica coloca desafios à teoria do dano: embora cause prejuízos difusos à ordem social e aos direitos fundamentais (como o direito à informação verídica), nem sempre haverá, no plano da responsabilidade civil clássica, um ilícito claramente atribuível a um agente e um dano concreto, direto e individualmente aferível. Essa constatação abre caminho para respostas jurídicas complementares, seja por meio de ações coletivas visando à tutela de interesses difusos, seja através de regulação específica do ambiente informacional digital, tema que será examinado adiante.

5.4 Análise de jurisprudência nacional e estrangeira sobre responsabilidade digital

A evolução jurisprudencial contemporânea demonstra o esforço dos tribunais, tanto no Brasil quanto no exterior, em adaptar os institutos tradicionais da responsabilidade civil aos novos desafios da era digital. A crescente utilização de sistemas de inteligência artificial e *chatbots* em serviços públicos e privados tem colocado à prova os limites da imputação de responsabilidade diante de informações incorretas, fraudulentas ou discriminatórias fornecidas por tais tecnologias. Nesse contexto, a jurisprudência cumpre papel essencial ao delinear os contornos da responsabilidade civil digital, fundada na boa-fé, no dever de informação e na reparação integral dos danos causados.

No âmbito nacional, verifica-se o entendimento consolidado de que as empresas que utilizam sistemas automatizados continuam responsáveis pelos atos e omissões decorrentes de seu funcionamento. O Superior Tribunal de Justiça (STJ) já reconheceu, em decisão paradigmática, que as instituições financeiras são

objetivamente responsáveis por falhas na prestação de serviços, mesmo quando estas decorrem de uso de tecnologias automatizadas.

Em Recurso Especial n. 1010322-67.2018.8.26.0152/SP, relatado pela Ministra Maria Thereza de Assis Moura, o STJ manteve acórdão do Tribunal de Justiça de São Paulo que condenara banco por não evitar fraude praticada por terceiros, ressaltando que a instituição possuía tecnologia suficiente para prevenir o ilícito, "inclusive com utilização de inteligência artificial para detecção do perfil do consumidor e da transação realizada". A decisão reforça que o uso de IA não exime o fornecedor do dever de vigilância e segurança previsto no art. 14 do Código de Defesa do Consumidor.

Na mesma linha, o Tribunal de Justiça de Minas Gerais (TJMG) reconheceu, em Agravo de Instrumento n. 1.0000.20.597631-9/001, relatado pelo Desembargador Marcos Henrique Caldeira Brant, a responsabilidade de uma empresa por exclusão automática de conta comercial em aplicativo de mensagens sem prévia justificativa. O acórdão asseverou que "*diversas medidas adotadas em ambientes digitais advêm de decisões tomadas por máquinas mediante a aplicação de algoritmos*", sendo dever das empresas responder pelas decisões de suas máquinas e sistemas. Assim, o tribunal consolidou o entendimento de que a automação não rompe o nexo de imputação entre o agente econômico e o dano gerado pelo sistema que ele próprio desenvolve ou utiliza.

Outros tribunais estaduais têm igualmente afirmado a responsabilização de empresas tecnológicas por danos decorrentes de seus sistemas algorítmicos. No processo n. 0816292-73.2020.8.10.0001, o Tribunal de Justiça do Maranhão (TJMA) condenou a empresa responsável pelo aplicativo TikTok pelo uso indevido de ferramenta de reconhecimento facial que coletava dados biométricos sem consentimento informado, violando a Lei Geral de Proteção de Dados (LGPD) e o direito à privacidade. A sentença reconheceu a existência de dano moral coletivo e impôs multa de R$ 23 milhões, consolidando o entendimento de que o tratamento automatizado de dados sensíveis exige transparência e consentimento explícito.

Em caso análogo, o Tribunal de Justiça de São Paulo (TJSP) responsabilizou a operadora Vivo por importunar consumidores com ligações automatizadas de telemarketing. No processo n. 1022312-33.2022.8.26.0114, a juíza Renata Oliva B. de Souza entendeu que o uso abusivo de robôs de contato viola o princípio da boa-fé

objetiva e enseja dano moral, aplicando a teoria do desvio produtivo do consumidor, segundo a qual o tempo desperdiçado para conter a prática abusiva configura lesão indenizável.

No campo da proteção de dados e da informação verídica, o STJ consolidou entendimento de que a inscrição indevida em cadastros de crédito gera dano moral presumido (*in re ipsa*), ainda que derivada de erro automatizado, conforme precedentes que originaram a Súmula 385. Tais decisões evidenciam o reconhecimento de que o avanço tecnológico não elimina o dever de reparação civil, mas, ao contrário, reforça o dever de cautela e supervisão humana sobre os sistemas automatizados.

No plano internacional, observa-se que as cortes estrangeiras têm avançado na construção de parâmetros próprios de responsabilidade digital. Nos Estados Unidos, o caso Mark Walters v. OpenAI LLC (Superior Court of Gwinnett County, Geórgia, 2025) foi o primeiro processo de difamação envolvendo um chatbot de IA. O autor alegou que o sistema ChatGPT havia produzido uma resposta difamatória, imputando-lhe falsamente envolvimento em desvio de verbas. A corte, porém, rejeitou o pedido por ausência de dolo ou negligência, reconhecendo que a empresa adota “esforços líderes na indústria” para reduzir erros e alerta os usuários sobre imprecisões. A decisão, embora favorável à OpenAI, inaugura debate sobre os limites da responsabilidade de desenvolvedores de IA generativa.

Ainda nos Estados Unidos, o caso Garcia v. Character Technologies Inc. (U.S. District Court, M.D. Florida, 2025) discute a morte de um adolescente supostamente influenciado por chatbot da empresa Character.AI. A ação questiona se a comunicação automatizada pode ser considerada discurso protegido pela Primeira Emenda, levantando debate sobre a eventual “liberdade de expressão” de sistemas de IA. O resultado do processo poderá redefinir as fronteiras entre regulação e liberdade informacional no contexto digital norte-americano.

No Canadá, o precedente Jake Moffatt v. Air Canada (Civil Resolution Tribunal, 2024) firmou marco inédito de responsabilidade civil por informação incorreta fornecida por chatbot. O tribunal entendeu que a companhia aérea não poderia alegar que o chatbot era “entidade separada”, afirmando que “*é óbvio que a Air Canada é responsável por todas as informações em seu site*”. A decisão consolidou a

responsabilidade do fornecedor pelas declarações automatizadas emanadas de suas plataformas digitais.

Na Europa, o caso NJCM et al. v. Netherlands (SyRI), julgado pelo Tribunal Distrital de Haia em 5 de fevereiro de 2020, declarou ilegal o sistema estatal SyRI (System Risk Indication) por violação ao direito à privacidade e ao princípio da transparência previstos na Convenção Europeia de Direitos Humanos. O tribunal considerou que o SyRI realizava tratamento discriminatório e desproporcional de dados pessoais, afetando desigualmente populações vulneráveis. A decisão tornou-se paradigma internacional ao afirmar que a eficiência algorítmica não pode se sobrepor a direitos fundamentais, sobretudo quando há opacidade nos critérios de decisão automatizada.

De forma convergente, constata-se que, no Brasil e no exterior, as cortes têm reafirmado que a utilização de inteligência artificial não rompe o vínculo de responsabilidade entre o agente e o dano causado. A automação, portanto, não constitui causa excludente de ilicitude, mas impõe maiores deveres de diligência, segurança e transparência.

Assim, a jurisprudência contemporânea reforça que o desenvolvimento tecnológico deve submeter-se aos valores da dignidade da pessoa humana, da boa-fé objetiva e do acesso à informação correta, pilares essenciais do Estado Democrático de Direito.

6 DESAFIOS REGULATÓRIOS E PERSPECTIVAS FUTURAS

A inovação tecnológica impulsionada pelos avanços em IA, impõe ao Direito um desafio, visando a construção de regulação que seja, aptos a fomentar o progresso e a proteger direitos fundamentais. A defasagem temporal entre o desenvolvimento de novas tecnologias e a capacidade de resposta do legislador cria um ambiente de insegurança jurídica, no qual os institutos tradicionais são constantemente questionados por novas realidades, como a tomada de decisão autônoma, a ocultação algorítmica e a coleta de dados.

A regulação do mundo digital exige uma abordagem multifacetada, que transcenda as fronteiras nacionais e dialogue com diferentes áreas do conhecimento. A complexidade dos sistemas de IA e seus impactos sistêmicos demandam soluções que equilibrem a inovação com a responsabilidade (accountability), a liberdade econômica com a proteção do indivíduo e a eficiência com a equidade.

Nesse sentido, enquanto marcos regulatórios específicos para a IA ainda se encontram em fase de maturação, normas já consolidadas servem como balizas essenciais, ao mesmo tempo que se discutem novos paradigmas para a atribuição de deveres e a alocação de riscos.

Este capítulo final se propõe a explorar o panorama dos desafios regulatórios e a delinear as perspectivas futuras para a governança da tecnologia. A análise será iniciada pela aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) como um instrumento já vigente para a imposição de limites ao tratamento de dados.

Em seguida, será ampliado para as iniciativas legislativas, tanto no Brasil quanto no cenário internacional, que buscam criar um regime jurídico específico para a IA reconhecendo que a regulação não se esgota na lei, e sim abrangendo os princípios éticos e dos modelos de governança algorítmica.

Por fim, o capítulo abordará a fronteira do pensamento jurídico na área, discutindo propostas inovadoras de responsabilização que buscam se adaptar à era digital.

6.1 A Lei Geral de Proteção de Dados (LGPD) e os limites do uso de dados pessoais

A Lei nº 13.709/2018 – Lei Geral de Proteção de Dados (LGPD) – inaugurou no Brasil um regime abrangente de proteção da privacidade, impondo obrigações estritas para o tratamento de dados pessoais. No contexto da inteligência artificial (IA), a LGPD estabelece balizas legais importantes quanto ao uso de dados por sistemas automatizados.

Primeiramente, a LGPD consagra princípios-chave como a finalidade específica e a adequação do tratamento, exigindo que os dados pessoais coletados para um determinado propósito não sejam posteriormente utilizados de forma incompatível com aquela finalidade original (art. 6º, I e II da LGPD).

Assim, algoritmos de IA devem respeitar limites claros de utilização dos dados, vinculados ao consentimento dado pelo titular e às finalidades informadas no momento da coleta (ou a outra base legal adequada) – condição essencial para legitimar o tratamento e garantir a transparência e lealdade no uso das informações.

O consentimento, quando exigido, deve ser livre, informado e específico, permitindo ao indivíduo conhecer de antemão a que se destinam seus dados e manifestar concordância de forma explícita; tal requisito busca concretizar o direito do usuário de saber como suas informações serão empregadas, reforçando sua autonomia sobre dados pessoais (SILVA; MUNIZ, 2023, p. 118).

Em suma, a LGPD impõe limites legais ao uso de dados em sistemas de IA na medida em que exige finalidades legítimas e explícitas, bem como garante aos titulares um conjunto de direitos que visam dar transparência e controle sobre seus dados, prevenindo abusos e usos desproporcionais das informações coletadas.

Um dos desafios centrais é conciliar a opacidade técnica de muitos algoritmos de IA com o princípio da transparênciae o direito de informação assegurado pela LGPD. Sistemas de aprendizado de máquina complexos frequentemente operam como verdadeiras “*caixas-pretas*”, nas quais nem mesmo os desenvolvedores conseguem explicar com precisão o critério de tomada de decisões.

Esse caráter opaco contrasta com as obrigações de transparência e explicabilidadeimpostas pela LGPD e pela regulamentação de dados pessoais em geral – obrigações essas que visam permitir que os titulares compreendam, ao menos em linhas gerais, como e por que determinadas decisões automatizadas foram tomadas.

A LGPD, inspirada no Regulamento Geral de Proteção de Dados europeu (GDPR), contempla expressamente o direito à revisão de decisões automatizadas que afetem os interesses do cidadão (art. 20). Esse dispositivo garante ao titular dos dados o direito de solicitar que decisões tomadas unicamente por algoritmos sejam revistas por uma pessoa natural, assegurando também o acesso a informações claras sobre os critérios e os procedimentos utilizados pelo sistema automatizado.

Trata-se, em essência, do reconhecimento de um “direito à explicação” das decisões algorítmicas no âmbito da proteção de dados, o que impõe limites importantes à atuação de inteligências artificiais em atividades que produzam efeitos jurídicos ou significativos sobre os indivíduos.

Conforme observado por PEREIRA, 2025, p. 90, a LGPD estabelece direitos fundamentais como o direito à explicação e à revisão de decisões automatizadas, justamente para resguardar os titulares diante da falta de transparência de muitos sistemas de IA.

Na prática, porém, efetivar esse direito enfrenta obstáculos técnicos: a capacidade de explicar decisões de certos modelos de IA (como redes neurais profundas) ainda está em estágios iniciais de desenvolvimento, demandando esforços de pesquisa em IA explicável (XAI) e possivelmente regulamentações específicas para torná-lo exequível.

Outro aspecto crítico abarcado pela LGPD é o princípio da não discriminação (art. 6º, IX), diretamente relevante no contexto de algoritmos de IA. Sistemas automatizados podem, inadvertidamente, replicar e até amplificar vieses discriminatórios presentes nos dados de treinamento ou nas instruções fornecidas, levando a resultados injustos para certos grupos sociais (por exemplo, recusas de

crédito desproporcionalmente altas para minorias, análises tendenciosas em processos seletivos automatizados, etc.).

A LGPD não menciona explicitamente "*inteligência artificial*" ou "*algoritmos*" em seu texto; ainda assim, suas diretrizes amplas – incluindo os princípios de transparência, segurança, prevenção e não discriminação – incidem sobre qualquer processamento automatizado de dados pessoais em larga escala. Isso significa que, sempre que um sistema de IA utilizar dados pessoais em suas operações, estará sujeito às regras da LGPD (mesmo que a lei não trate nominalmente de IA), devendo respeitar, por exemplo, a qualidade dos dados (para evitar que informações desatualizadas ou incorretas gerem decisões enviesadas) e não podendo utilizar dados sensíveis para fins discriminatórios ilícitos.

A preocupação com a discriminação algorítmica tem destaque tanto na literatura jurídica quanto nas diretrizes internacionais: algoritmos podem refletir preconceitos históricos e produzir impactos negativos a direitos fundamentais.

Por isso, o arcabouço da LGPD – aliado a outros diplomas, como o Código de Defesa do Consumidor e a legislação antidiscriminatória – funciona como um freio jurídico ao uso indiscriminado de dados em IA, ao vedar tratamentos que resultem em discriminações injustificadas e exigir do controlador diligência na mitigação de vieses.

Em síntese, os limites legais para uso de dados pessoais por sistemas de IA, estabelecidos pela LGPD, abrangem desde exigências procedimentais (consentimento adequado, definição de finalidade, medidas de segurança) até garantias substantivas (direito à privacidade, à não discriminação e à explicação de decisões automatizadas), compondo um quadro normativo que busca equilibrar a inovação algorítmica com a proteção dos direitos da personalidade e da igualdade.

No entanto, persistem desafios jurídicos e práticos para a plena efetividade dessas salvaguardas no contexto da IA. A rápida evolução tecnológica e a complexidade técnica criam uma espécie de "brecha" entre as normas existentes e a realidade do uso massivo de dados por sistemas inteligentes.

Por exemplo, garantir transparência em modelos de aprendizado profundo exige não apenas disposição legal, mas também ferramentas técnicas de auditoria

algorítmica e conhecimento especializado – recursos que nem sempre estão disponíveis às autoridades e aos titulares dos dados.

A Autoridade Nacional de Proteção de Dados (ANPD), órgão responsável por fiscalizar o cumprimento da LGPD, enfrenta limitações de ordem técnica, humana e orçamentária que podem comprometer sua capacidade de supervisionar sistemas de IA de alta complexidade. Isso levanta preocupações sobre a efetividade do enforcement: sem uma estrutura robusta de fiscalização, os direitos assegurados pela LGPD – como a revisão de decisões automatizadas ou a reparação por uso indevido de dados – podem restar apenas no papel.

Ademais, a LGPD impõe obrigações genéricas (aplicáveis a todos os setores), enquanto a IA apresenta características sui generis que demandam interpretações específicas. Questões como a definição do que constitui uma decisão automatizada relevante, ou até que ponto é exigível a explicação técnica de um algoritmo sem violar segredos comerciais, são dilemas em aberto na aplicação da LGPD à IA.

Assim, embora a LGPD forneça um marco legal fundamental para delimitar o uso de dados pessoais por inteligências artificiais – enfatizando consentimento, finalidade, transparência, segurança e não discriminação –, a sua implementação nesse campo requer uma abordagem complementar: desenvolvimento de normas setoriais e técnicas, fortalecimento das capacidades das autoridades e conscientização dos agentes de tratamento sobre os riscos de práticas algorítmicas abusivas.

Somente com essa conjugação de esforços será possível assegurar que a revolução da IA no Brasil ocorra em conformidade com os direitos fundamentais à privacidade e à igualdade, prevenindo excessos e protegendo a dignidade dos titulares dos dados em face de decisões automatizadas.

6.2 Iniciativas legislativas brasileiras e internacionais para regulação da IA

Diante dos desafios apontados, o ordenamento brasileiro vem buscando formular um marco regulatório específico para a inteligência artificial, complementando as normas gerais já existentes (como a LGPD e o Marco Civil da Internet). Nos últimos

anos, diversas proposições legislativas emergiram no Congresso Nacional visando disciplinar o desenvolvimento e o uso de sistemas de IA.

A principal delas é o Projeto de Lei nº 2.338/2023, em tramitação desde 2023, que representa uma tentativa abrangente de regular a IA no país. O PL 2.338/2023 alinha-se explicitamente ao modelo europeu emergente, tomando como referência o projeto do Artificial Intelligence Act da União Europeia. Assim como o regulamento europeu, o PL brasileiro adota uma classificação de risco para as aplicações de IA – categorizando-as em níveis como risco mínimo, limitado, alto e inaceitável – e prevê obrigações proporcionais ao grau de risco de cada sistema. Por exemplo, sistemas de "alto risco" (a serem definidos em regulamento) teriam de observar requisitos mais estritos de transparência, gestão de riscos, governança de dados e, possivelmente, submissão a avaliação de conformidade antes da entrada em operação.

Já aplicações consideradas de risco mínimo ou meramente acessórias sofreriam pouca ou nenhuma intervenção regulatória direta, preservando um espaço para inovação. A inspiração europeia é nítida e, em tese, positiva ao dotar o Brasil de uma estrutura normativa moderna, capaz de abordar fenômenos como sistemas de reconhecimento facial, algoritmos preditivos em saúde ou finanças, e mesmo inteligências generativas, de acordo com seu potencial lesivo ou disruptivo.

Contudo, especialistas apontam que a simples transposição do modelo do EU AI Act sem as devidas adaptações pode ser problemática. O PL 2.338/2023 já recebe críticas por certa falta de precisão conceitual e por indefinições institucionais – como não indicar claramente qual órgão será a autoridade central responsável pela regulação e fiscalização da IA.

Além disso, ressalta-se que o projeto importa categorias e terminologias do direito europeu que podem não se adequar plenamente à realidade brasileira, marcada por desigualdades regionais em acesso à tecnologia, baixa capacitação técnica em muitos setores e carência de infraestrutura digital em áreas menos desenvolvidas (fatores que diferenciam o cenário brasileiro do contexto médio europeu).

Em paralelo ao PL 2.338/2023, outras iniciativas têm sido discutidas – a Estratégia Brasileira de Inteligência Artificial (EBIA), lançada em 2021, estabeleceu diretrizes éticas e de fomento à IA (ainda que de natureza programática e não vinculante) em consonância com princípios internacionais como os da OCDE.

No âmbito setorial, órgãos como o Conselho Nacional de Justiça editaram normativas próprias (v.g., a Resolução CNJ n. 332/2020) disciplinando o uso de IA no Poder Judiciário, o que demonstra um movimento interno de autorregulação enquanto a lei geral não é aprovada (BRAGA; PEREZ FILHO, 2025, p. 109).

Observa-se, enfim, um cenário legislativo em ebulição, com propostas concorrentes e complementares: desde projetos de lei mais principiológicos e voltados a direitos (como o PL 21/2020, que tramitou anteriormente) até esse novo PL 2.338/2023 de caráter mais regulatório-técnico.

A tendência atual converge para a consolidação deste último como base do Marco Legal da IA no Brasil, incorporando a abordagem de regulação por níveis de risco e prevendo mecanismos de governança, supervisão e incentivo à inovação responsiva.

No contexto internacional, as iniciativas de regulação da IA também se multiplicaram, embora sigam abordagens distintas conforme os valores e estruturas de cada jurisdição. Na União Europeia, avança o trâmite do chamado AI Act, uma legislação pioneira que deverá ser implementada progressivamente até 2026.

O AI Act europeu caracteriza-se por proibir certas utilizações de IA consideradas intoleráveis (como sistemas de vigilância massiva em tempo real ou mecanismos de pontuação social nos moldes chineses) e regular estritamente as aplicações de alto risco, impondo-lhes requisitos de conformidade técnica, documentação, transparência e supervisão humana (BELLI; CURZI; GASPAR, 2023, p. 74).

Por exemplo, um algoritmo usado em seleção de emprego ou em diagnóstico médico – áreas sensíveis envolvendo direitos fundamentais – precisará cumprir obrigações de gestão de risco, manter registros auditáveis e oferecer informações claras às pessoas impactadas, inclusive quanto à possibilidade de intervenção humana e contestação de resultados.

Já aplicações de risco limitado deverão seguir códigos de conduta ou normas técnicas voluntárias, enquanto as de risco mínimo ficam fora do escopo regulatório para não sufocar inovações benignas. Essa proposta europeia reflete a visão de que a regulação da IA deve colocar os direitos humanos no centro, garantindo que valores como privacidade, não discriminação, transparência e segurança estejam resguardados (CHAVES, 2024, p. 83).

Não por acaso, a UE também atualizou outros marcos para complementar o AI Act – como a Diretiva de Responsabilidade Civil para IA e discussões sobre requisitos de explicabilidade e governança de dados. Esse movimento europeu tem sido observado com atenção no Brasil: estudos sugerem que o país pode se beneficiar ao seguir exemplos da UE no tocante à proteção de dados e transparência algorítmica, adaptando aquelas lições ao nosso ordenamento.

Por sua vez, os Estados Unidos adotam, até o momento, uma estratégia mais flexível e fragmentada. Em nível federal, não há até 2025 uma lei geral de IA; a abordagem norte-americana apoia-se em marcos setoriais e na autorregulação de mercado, com foco na inovação. Documentos orientativos, entretanto, têm emergido: destaca-se o Blueprint for an AI Bill of Rights (lançado pelo governo dos EUA em 2022) com princípios para uso ético da IA, e o Framework de Gerenciamento de Riscos de IA do NIST (2023), que oferece diretrizes técnicas para identificar e mitigar riscos algorítmicos.

O framework do NIST propõe um modelo voluntário de governança de IA centrado em quatro funções (governar, mapear, mensurar e gerenciar riscos), buscando compatibilidade com padrões internacionais e servindo de referência para empresas adotarem boas práticas.

Entretanto, a ausência de obrigatoriedade legal desse esquema faz com que a eficácia dependa da adesão espontânea das empresas e do escrutínio ex post por agências reguladoras setoriais (como FDA, FTC, etc.). Há um debate contínuo nos EUA sobre a necessidade de legislação federal específica, mas até então prevalece um modelo híbrido de soft law e normas existentes, sob o argumento de não tolher a competitividade tecnológica americana (YEUNG, 2019, p. 85).

Outros países oferecem contrastes interessantes. A China segue uma via singular, implementando o que se poderia chamar de modelo estatal-centralizado de regulação da IA. Diferentemente das democracias ocidentais, a governança chinesa da IA é verticalizada e de caráter autoritário, conduzida por agências governamentais como a Administração do Ciberespaço da China (CAC) em estreita coordenação com as grandes empresas de tecnologia domésticas.

Nos últimos anos, a China editou normas específicas impondo controles rigorosos: por exemplo, o regulamento sobre algoritmos de recomendação (que obriga plataformas a registrar seus algoritmos junto ao governo e oferece aos usuários opções para desligar recomendações personalizadas) e as diretrizes sobre IA generativa (exigindo aprovação estatal para modelos generativos de grande porte, bem como responsabilidade das empresas pelos conteúdos gerados).

A lógica subjacente é proteger a segurança nacional e a estabilidade social, evitando que a IA se torne vetor de dissensão política ou desordem social – o que resulta em forte censura e monitoramento, mas também em estímulos para o desenvolvimento de tecnologias “soberanas” chinesas (como algoritmos alinhados aos valores do Partido e padrões nacionais).

Esse modelo chinês, embora bem-sucedido em impulsionar a liderança da China em patentes e aplicações de IA, suscita críticas quanto à falta de transparência e ao desrespeito a direitos individuais de privacidade e liberdade de expressão, ilustrando um dilema entre progresso tecnológico e garantias civis (AMORIM; SILVA, 2023, p. 93). Já em democracias liberais de médio porte, há experiências diversas: o Canadá e o Japão enfatizam a elaboração de princípios éticos e guias de boas práticas (soft law) como primeiro passo; o Reino Unido optou por não criar uma agência única de IA, preferindo distribuir orientações entre reguladores setoriais (saúde, transportes, finanças etc.), sob uma abordagem pro-inovação e de “orientação por resultados” em vez de regras rígidas ex ante (BRAGA; PEREZ FILHO, 2025, p. 109).

Em contraste, a União Europeia segue com normas rígidas (modelo “baseado em regras”), os EUA combinam elementos setoriais e autorregulação (modelo “híbrido”), e Singapura aparece como referência de modelo híbrido pragmático, mesclando incentivos à inovação com padrões de prestação de contas. Essas

iniciativas internacionais convergem ao reconhecer certos temas transversais: a necessidade de combater vieses algorítmicos e assegurar não discriminação; de promover transparência e explicabilidade nos sistemas de IA; de garantir *accountability* (responsabilização) pelos danos causados por inteligências artificiais; e de investir na capacitação técnica e educação para que sociedade e órgãos públicos possam acompanhar a evolução tecnológica.

Tais objetivos aparecem, por exemplo, nos Princípios da OCDE para IA (2019), endossados por dezenas de países (inclusive o Brasil), que recomendam que sistemas de IA sejam projetados em torno de valores como justiça, transparência, robustez e respeito aos direitos humanos, ao mesmo tempo em que ressaltam a importância de mecanismos de avaliação de risco e governança multidisciplinar.

Contudo, princípios isolados sem mecanismos de enforcement efetivo tendem a ter impacto limitado – fenômeno já criticado como "*ethics washing*", quando empresas ou governos adotam cartas de princípios éticos apenas para melhorar sua imagem, sem mudanças concretas nas práticas.

Diante desse cenário, ganha força a busca por modelos regulatórios híbridos, que combinem o melhor dos dois mundos: regulação estatal (hard law) suficiente para garantir direitos e segurança jurídica, e instrumentos flexíveis (soft law)capazes de acompanhar a rápida evolução tecnológica sem engessar a inovação.

Essa proposta de convergência pode ser percebida tanto na doutrina quanto nas políticas recentes. (AMORIM; SILVA, 2023, p. 93) defendem que modelos normativos puramente principiológicos são insuficientes se não acompanhados de mecanismos concretos de aplicação e estruturas adaptativas de regulação.

Por outro lado, a hiper-regulamentação pode sufocar o desenvolvimento econômico e tecnológico ou rapidamente se tornar obsoleta frente a novas descobertas. Assim, delineia-se um consenso de que é necessário conciliar a inovação tecnológica com garantias éticas e jurídicas, o que implica arquitetar uma governança compartilhada entre Estado, iniciativa privada, academia e sociedade civil. Na prática, um modelo híbrido de regulação da IA envolveria: (i) legislação básica estabelecendo direitos, deveres e limites claros (por exemplo, proibindo discriminação

algorítmica, assegurando direito a contestar decisões automatizadas, exigindo avaliações de impacto em sistemas de alto risco); (ii) agências reguladoras ou autoridades administrativas especializadas dotadas de competência para expedir normas técnicas complementares, fiscalizar e aplicar sanções – no caso brasileiro, discute-se se a ANPD seria essa autoridade para IA ou se caberia criar um novo órgão regulador específico (o PL 2.338/2023, por ora, delega a função à ANPD e órgãos setoriais, o que tem sido questionado pela potencial falta de coordenação); (iii) mecanismos de auto e co-regulação fomentados pelo Estado, como códigos de conduta para desenvolvedores, certificações voluntárias de algoritmos confiáveis, seal of ethics para empresas aderentes a boas práticas, entre outros; e (iv) ferramentas regulatórias inovadoras, a exemplo dos regulatory sandboxes, que permitem experimentação supervisionada de soluções de IA em ambientes controlados.

Essas ferramentas – já testadas no Brasil nos setores financeiro e de saúde suplementar – viabilizam que empresas e órgãos públicos desenvolvam projetos-piloto de IA sob acompanhamento próximo do regulador, ajustando requisitos conforme os resultados e aprendizados obtidos.

A literatura também destaca a importância de auditorias algorítmicas independentes e da participação social na governança da IA (por meio de conselhos, consultas públicas e envolvimento de grupos potencialmente afetados), de modo a conferir legitimidade e eficácia às medidas adotadas (PEREIRA; DIAS; GIANORDOLI, 2025, p. 97).

Em síntese, a regulação efetiva da IA não se esgota na edição de uma lei – ela exige a construção de um ecossistema adaptativo de governança, com múltiplas camadas e atores (BRAGA; PEREZ FILHO, 2025, p. 109). Somente com esse arranjo híbrido será possível enfrentar os desafios transversais da IA – como vieses, opacidade e responsabilidade – sem bloquear os benefícios da inovação. No caso brasileiro, esse equilíbrio ainda está em construção: a aprovação do marco legal (PL 2.338/2023) será um passo importante, mas sua eficácia dependerá da harmonização com normas existentes (e.g. LGPD), do fortalecimento institucional para enforcement e da contínua atualização das regras conforme a tecnologia evolui.

Em última análise, tanto no Brasil quanto no exterior, conciliar desenvolvimento tecnológico com garantias éticas e jurídicas tornou-se o imperativo central da regulação da IA – um objetivo que demanda soluções criativas, cooperação internacional e um compromisso firme com a proteção dos direitos fundamentais na era da inteligência artificial.

6.3 Princípios éticos e modelos de governança algorítmica

A rápida difusão da Inteligência Artificial nas últimas décadas suscitou diversas iniciativas voltadas a estabelecer fundamentos éticos para seu desenvolvimento e uso responsável. Princípios orientadores como transparência, equidade, *accountability* (prestação de contas), não discriminação, privacidade, segurança e sustentabilidade emergem como pilares nos relatórios e diretrizes internacionais sobre IA.

Desde o fim da década de 2010, organismos globais como a OCDE e a UNESCO propuseram frameworks éticos que colocam a dignidade humana, a transparência e a responsabilidade no centro da governança da IA. Esses documentos – de natureza principiológica – buscam assegurar que a tecnologia respeite valores fundamentais e os direitos humanos.

Por exemplo, a Estratégia da UNESCO para IA identificou valores como inclusão, bem-estar, respeito à autonomia e não maleficência, alinhando-se a esse consenso global. Da mesma forma, pesquisadores nacionais têm destacado um conjunto de princípios básicos cuja observância reduz riscos de vieses e abusos: responsabilidade, explicabilidade, proteção de dados, justiça e equidade, liberdade e supervisão humana, além dos já citados transparência e segurança. Tais princípios éticos operam como diretrizes para desenvolver algoritmos de forma a mitigar discriminações e permitir escrutínio público.

Conforme ressalta PESSOA, 2024, p. 42-47, a aplicação consistente desses princípios, aliada à existência de regulamentações claras, é crucial para uma governança algorítmica eficaz, capaz de reduzir vieses e promover a confiança nos sistemas de IA (PESSOA, 2024, p. 42-47).

Entretanto, os princípios éticos, por si sós, enfrentam limites práticos caso não sejam acompanhados de mecanismos robustos de governança e enforcement regulatório. Estudos críticos apontam que meras declarações de boa intenção – embora relevantes como ponto de partida – podem carecer de efetividade jurídica. (AMORIM; SILVA, 2023, p. 4) observam que abordagens puramente principiológicas sofrem de *baixa capacidade de enforcement* e tendem a negligenciar assimetrias estruturais entre os atores envolvidos.

Em outras palavras, sem instrumentos concretos de supervisão e responsabilização, princípios gerais correm o risco de se tornarem retórica vazia, especialmente diante do poder opaco dos algoritmos nas sociedades atuais. Nesse sentido, diversos autores defendem a necessidade de se avançar de códigos de ética voluntários para modelos de governança algorítmica institucionalizados, com regras claras de transparência algorítmica, auditoria independente e prestação de contas.

A esse respeito, LIMA, 2023, p. 118-127 propõem uma perspectiva humanista e crítica da governança de algoritmos, enfatizando a centralidade da autonomia individual, da dignidade humana e do controle democrático sobre sistemas automatizados. A transparência dos processos decisórios automatizados e a possibilidade de revisão humana de decisões algorítmicas são frequentemente citadas como requisitos éticos básicos para que a IA esteja alinhada com valores democráticos. (FLORIDI, 2014, p. 74; ROUVROY, 2013, p. 186, LIMA, 2023, p. 289-391).

Desse modo, a convergência entre princípios éticos e mecanismos de governança torna-se indispensável: princípios fornecem a direção normativa, enquanto a governança algorítmica cria as estruturas para concretizá-los e fiscalizar seu cumprimento.

No cenário internacional, diferentes modelos de governança algorítmica têm sido adotados, refletindo prioridades regulatórias e valores sociopolíticos distintos. União Europeia, Estados Unidos, China e Reino Unido figuram entre os paradigmas mais influentes, cada qual exemplificando abordagens próprias de regulação da IA.

A União Europeia destaca-se por uma postura proativa e normativa, centrada na proteção de direitos fundamentais e na regulação ex ante dos riscos da IA. O bloco europeu tem desenvolvido um extenso marco regulatório (como o *Artificial Intelligence Act,* em vias de aprovação) que classifica os sistemas de IA por níveis de risco e impõe obrigações proporcionais – incluindo requisitos rigorosos de transparência, gestão de dados e controle humano para sistemas de alto risco.

Esse modelo europeu pauta-se pelo princípio da precaução e pela tutela da segurança, não discriminação e privacidade dos cidadãos, refletindo a tradição europeia de regulação dirigida por direitos. Em contraste, os Estados Unidos adotam até o momento uma abordagem mais descentralizada e guiada pelo mercado. Não há uma lei federal abrangente sobre IA; a governança apoia-se em instrumentos soft law, padrões técnicos e ações de agências setoriais.

Documentos como o *Blueprint for an AI Bill of Rights* escrita pela Casa Branca, 2022 e o *NIST AI Risk Management Framework* oferecem diretrizes éticas e de gerenciamento de riscos, porém sem força vinculante. Essa estratégia estadunidense privilegia a autorregulação e a inovação, visando não tolher o desenvolvimento tecnológico – uma abordagem alinhada à tradição liberal de responsabilidade ex post e intervenção estatal mínima (DOURADO & AITH, 2022; PEREIRA, 2025, p. 2-6).

Já a China envereda por um caminho praticamente oposto: sua governança de IA é centralizada e verticalizada, com forte atuação do Estado no controle algorítmico. Regulamentos emanados pela Administração do Ciberespaço da China e outros órgãos impõem restrições estritas, exigindo que algoritmos sigam valores socialista e prevenindo usos considerados nocivos à ordem pública, como proibições a algoritmos que disseminem informação ilegal ou ferham a moral pública.

Trata-se de um modelo focado em regras detalhadas e censura preventiva, no qual a IA é vista como questão de segurança nacional e estabilidade social (AMORIM; SILVA, 2023, p. 4). Por fim, o Reino Unido adota uma postura intermediária: fora da UE, optou por um modelo flexível baseado em resultados, sem uma lei geral de IA, mas emitindo princípios orientadores para que reguladores setoriais apliquem às diferentes indústrias (estratégia *pro-innovation*, 2023).

Cada uma dessas abordagens internacionais ilustra um dilema chave da governança algorítmica: equilibrar inovação tecnológica com proteção de direitos.

Portanto, enquanto UE e China representam polos de maior intervenção regulatória (a primeira voltada a direitos, a segunda ao controle estatal), os EUA e, em menor grau, o Reino Unido apostam em autorregulação e em ajustes pontuais, confiando na responsabilidade dos agentes de mercado e nos mecanismos tradicionais de responsabilidade civil para lidar com eventuais abusos.

O Brasil, diante desse panorama global, enfrenta o desafio de construir seu modelo próprio de governança da IA, aprendendo com as experiências estrangeiras mas atendendo às peculiaridades locais. Nos últimos anos, o país deu passos iniciais importantes, embora ainda não possua uma legislação específica consolidada sobre IA.

Em 2021 foi publicada a Estratégia Brasileira de Inteligência Artificial (EBIA), a qual enunciou princípios éticos alinhados às diretrizes da OCDE – tais como crescimento inclusivo, inovação responsável, respeito aos direitos humanos, transparência e prestação de contas (*accountability*). Todavia, conforme destaca AMORIM & SILVA, 2023, p. 3, a EBIA possui natureza programática e não vinculante, servindo mais como orientação de políticas do que imposição jurídica concreta. Na ausência de força obrigatória, persistem dúvidas sobre sua efetividade prática.

Paralelamente, tramitaram no Congresso Nacional alguns projetos de lei buscando estabelecer um marco regulatório para IA. O PL 21/2020 – primeiro texto de abrangência geral sobre IA no Brasil – propôs princípios e diretrizes para o desenvolvimento da IA. Apesar de seu mérito pioneiro, o PL 21/2020 recebeu críticas na comunidade jurídica pela tramitação apressada e pelo teor excessivamente genérico e sucinto (apenas 10 artigos).

Ele priorizava alguns princípios (como transparência e uso ético de sistemas automatizados), porém deixava lacunas em pontos fundamentais, como critérios de avaliação de riscos, fiscalização, responsabilização civil e sanções. Além disso, o regime de responsabilidade previsto originalmente no PL 21/2020 baseava-se na

lógica subjetiva (culpa), o que foi considerado inadequado dada a diversidade e complexidade das aplicações de IA.

Especialistas apontaram que insistir exclusivamente na culpa poderia transferir um ônus probatório desproporcional às vítimas dos danos algorítmicos, dificultando sua reparação (BELLI, CURZI; GASPAR, 2023, apud PEREIRA et al., 2025, p. 9-11). Esses pontos fracos motivaram o apensamento de outras proposições (PL 5051/2019, PL 872/2021) ao projeto principal e fomentaram debates para aperfeiçoar o texto legal.

Em 2023, ganhou destaque o Projeto de Lei nº 2338/2023, conhecido como o PL do Marco Legal da IA, que reflete uma evolução na abordagem regulatória brasileira. Esse projeto adota expressamente uma abordagem baseada em riscos e direitos, inspirada no modelo europeu do *AI Act*.

Pelo texto do PL 2338/23, sistemas de IA serão classificados conforme o grau de risco (por exemplo, alto risco em setores como saúde, transporte, crédito, etc.), sendo vedados aqueles de risco excessivo que atentem contra direitos fundamentais (v.g. sistemas de pontuação social ou de manipulação comportamental).

Obrigações mais rigorosas recaem sobre desenvolvedores e operadores de sistemas de maior risco – incluindo realização de avaliação de impacto algorítmico independente, requisitos de transparência e explicabilidade para usuários, e medidas de prevenção de viés e discriminação. Simultaneamente, o projeto assegura direitos aos indivíduos afetados por decisões automatizadas, tais como o direito à informação prévia de que se trata de IA, direito a explicação sobre a lógica da decisão, possibilidade de contestar decisões prejudiciais, além de proteção de dados e não discriminação algorítmica.

Importante notar que o PL 2338/2023 também enfrenta de frente a questão da responsabilização civil: ele estabelece a obrigação de reparar danos causados por sistemas de IA, atribuindo responsabilidade objetiva ao fornecedor ou operador nos casos de sistemas de alto risco (ou risco excessivo). Para sistemas de risco baixo ou médio, adota-se a culpa presumida do agente causador, invertendo-se o ônus da prova em favor da vítima.

Em outras palavras, o projeto combina regime de risco (objetivo) para IAs mais perigosas com um regime de falha presumida para as demais – solução híbrida que busca equilibrar proteção do lesado e incentivo à inovação. Até o momento, o PL 2338/2023 tem recebido emendas e passou por intensos debates no Senado, indicando tanto convergências com padrões internacionais quanto desafios políticos na sua aprovação.

Analistas consideram que sua implementação exigirá capacidade institucional para fiscalizar o cumprimento das obrigações e cooperação multissetorial para acompanhar a rápida evolução tecnológica (PEREIRA; DIAS; GIANORDOLI, 2025, p. 1-23).

Em suma, o Brasil se encontra num momento crucial de definição de seu modelo de governança algorítmica: há propostas avançadas em discussão, inspiradas nas melhores práticas internacionais (a exemplo da UE), porém será necessário enfrentar obstáculos como a falta de uma autoridade reguladora especializada, a definição clara de competências de fiscalização e a criação de incentivos para que empresas e órgãos públicos adotem efetivamente os princípios éticos e mecanismos de controle em suas aplicações de IA.

Somente com um arcabouço normativo efetivo, complementado por um ecossistema de governança adaptativo, será possível garantir que a IA no Brasil se desenvolva de forma inovadora sem comprometer direitos fundamentais, equacionando os objetivos de inovação e inclusão digital com a proteção da sociedade (BRAGA; PEREZ, 2025, p. 1-29).

6.4 Propostas de responsabilização adaptadas à era digital e aos agentes não humanos

O advento de agentes algorítmicos autônomos e dotados de capacidade de aprendizagem (*machine learning*) desafia os paradigmas clássicos da responsabilidade civil, exigindo uma releitura dos conceitos de culpa, nexo causal e sujeito responsável na era digital. Tradicionalmente, a responsabilidade civil se funda

na ideia de que, para haver obrigação de reparar um dano, é necessário identificar uma conduta humana culposa ou dolosa que tenha causado o prejuízo (teoria subjetiva baseada na culpa). Essa premissa, contudo, torna-se problemática diante da autonomia crescente dos sistemas de IA.

Como explica BARBOSA, 2020, p. 5-7, os sistemas inteligentes contemporâneos podem tomar decisões e evoluir de maneiras não previstas nem completamente compreendidas por seus programadores, o que dificulta traçar a fronteira entre um erro humano e um erro algorítmico.

A autora assinala que a centralidade da culpa nos modelos delituais clássicos revela-se insuficiente para lidar com danos causados por entes dotados de IA, pois "*as características de autonomia e autoaprendizagem de tais entes dificultam o traçar de fronteira entre os danos que resultam de um erro humano e aqueles que são devidos ao próprio algoritmo. O comportamento imprevisível deste, que decide por si como agir, [...] torna impossível conexionar um eventual dano [...] com uma conduta negligente do ser humano*" (BARBOSA, 2020, p. 5-7).

Em outras palavras, a opacidade algorítmica e a capacidade de decisão emergente dos algoritmos rompem o nexo de imputação subjetiva tradicional – muitas vezes não há um ato humano específico e intencional a ser apontado como causador direto do dano, já que a máquina atuou de forma semi-autônoma. Esse cenário gera o que alguns juristas denominam "lacuna de responsabilidade", isto é, a possibilidade de ocorrência de danos sem que se consiga atribuir, nos moldes clássicos, a responsabilidade a uma pessoa determinada (LOPES, 2020, p. 113-125).

Lopes analisa precisamente esse problema, notando que conforme agentes artificiais ganham maior autonomia decisória, surgem questionamentos quanto ao tratamento jurídico a ser conferido a tais agentes e à imputação de responsabilidade em caso de danos, sobretudo quando o prejuízo não pode ser diretamente atribuído a uma ação humana específica. A autora ressalta que se esses sistemas atuam independentemente das orientações diretas de seres humanos, é preciso repensar quem deve arcar com os custos dos eventuais danos por eles causados.

Assim, os modelos clássicos de responsabilidade – centrados na conduta humana culposa – mostram-se limitados frente à autonomia algorítmica, demandando teorias emergentes e adaptações legais para preencher essa lacuna e evitar zonas de irresponsabilidade na era digital.

Diante das limitações do paradigma tradicional de culpa, diversos juristas e formuladores de políticas têm proposto modelos alternativos de responsabilização de agentes não humanos. Uma das propostas mais difundidas é a adoção de regimes de responsabilidade objetiva (*strict liability*), baseados no risco da atividade, em vez de na culpa.

Nessa perspectiva, independe averiguar dolo ou negligência do agente: basta a ocorrência do dano ligado ao funcionamento do sistema de IA para surgir o dever de indenizar. A justificativa principal para esse modelo é protetiva – busca-se evitar que a vítima fique sem reparo devido à dificuldade de provar falha humana no caso de algoritmos complexos.

Na doutrina brasileira, ganha força a inclinação por aplicar a teoria objetiva aos danos de IA, por entendê-la mais adequada à tutela dos lesados. Como salientam Gustavo Tepedino e Rodrigo Silva, referidos por Lopes, o direito brasileiro já prevê cláusulas gerais de responsabilidade objetiva (como o art. 927, parágrafo único do CC, sobre atividade de risco) que podem abarcar atividades de IA, aliviando o ônus probatório das vítimas e facilitando a reparação.

De fato, há quem sustente que certas aplicações de IA devam ser qualificadas como "*atividades de risco*" por sua natureza potencialmente perigosa, atraindo a incidência direta da responsabilidade objetiva prevista em lei (art. 927, par. ún., CC). Exemplos frequentemente citados incluem veículos autônomos, cujo emprego massivo poderia deslocar a responsabilidade de acidentes para um âmbito objetivo: o simples fato do veículo automático causar dano implicaria dever de indenizar do fabricante ou operador, independentemente de comprovação de culpa.

Essa visão de responsabilidade pelo risco também inspira a proposta da União Europeia de uma Diretiva de Responsabilidade Civil para IA, que tende a adotar a inversão do ônus da prova em favor da vítima e padrões estritos de responsabilidade

especialmente para sistemas de alto risco (SILVA, 2024, apud PEREIRA et al., 2025, p. 6-7).

No Brasil, o PL 2338/2023 consagra expressamente essa opção política ao prever, como regra geral, a responsabilização do fornecedor ou operador de IA por danos causados, independentemente do grau de autonomia do sistema. Em casos de IA de alto risco, a responsabilidade do fornecedor/operador será objetiva; nos demais casos, haverá presunção de culpa do agente, com inversão do ônus da prova em benefício do prejudicado.

Segundo a exposição de motivos desse projeto, os legisladores brasileiros optaram por não criar novas teorias ad hoc, preferindo adaptar os institutos existentes de responsabilidade civil para cobrir os danos de IA – seja pelo caminho da objetivação do dever de reparar, seja pela distribuição dinâmica do ônus da prova (presunção legal de culpa).

Essa escolha reflete a confiança de que o arcabouço jurídico tradicional, devidamente reinterpretado, ainda pode solucionar grande parte dos litígios envolvendo inteligência artificial, sem necessidade de personalizar máquinas ou subverter os princípios basilares do direito civil.

Outra teoria emergente que ganhou notoriedade no debate jurídico foi a ideia de se conferir personalidade jurídica à inteligência artificial, criando a figura da "*pessoa eletrônica*". Essa proposta inusitada foi formalmente sugerida pelo Parlamento Europeu em 2017, quando aprovou uma resolução recomendando à Comissão Europeia avaliar a criação de um estatuto jurídico específico para robôs autônomos sofisticados, de modo que estes pudessem ser considerados "pessoas eletrônicas" responsáveis por reparar eventuais danos que causem.

A recomendação europeia – contida no princípio 59 (f) da Resolução 2015/2103 – partia do reconhecimento de que robôs com alto grau de autonomia decisória não se enquadram perfeitamente nas categorias jurídicas tradicionais (pessoas naturais ou bens), sugerindo uma terceira categoria para acomodá-los. Essa iniciativa gerou amplo debate doutrinário e reação de parte da comunidade científica.

De um lado, alguns autores viam na persona eletrônica uma solução para a lacuna de responsabilidade supracitada: ao dotar a IA de personalidade jurídica, ela se tornaria um sujeito de direito capaz de assumir obrigações e responder por danos com seu próprio patrimônio (ex.: um fundo vinculado ao robô) – analogamente ao que ocorre com as pessoas jurídicas empresariais.

Lopes explica que essa personificação não implicaria necessariamente atribuir à máquina todos os direitos de um ser humano, mas sim equipará-la a uma pessoa jurídica, como um centro de imputação de determinados direitos e deveres conforme sua natureza. Ou seja, seria uma ficção jurídica tal como são as sociedades e associações, criada por conveniência para responsabilizar entes não humanos.

Por outro lado, muitos juristas criticam fortemente a noção de pessoa eletrônica. NEGRI, 2020, p. 18-22 adverte que há um risco de antropomorfismo jurídico enganoso nessa metáfora sedutora de tratar robôs como “pessoas”. Segundo ele, equiparar máquinas a seres humanos, ainda que retoricamente, pode levar a distorções na atribuição de responsabilidade, desviando o foco das pessoas de carne e osso (fabricantes, programadores, usuários) para entes fictícios que, ao fim, não têm consciência nem patrimônio próprio suficientes.

Nesse sentido, se ampliar o conceito de personalidade a robôs não colocaria em risco a própria essência do conceito de humanidade: antes de conceder direitos ou status de pessoa a entes artificiais, seria necessário estudar profundamente o impacto disso sobre a distinção humano/máquina, para não banalizar aquilo que torna os humanos juridicamente especiais.

A autora sustenta que só seria admissível criar uma categoria de pessoa não humana (eletrônica) após criteriosos testes e comprovação de que essa mudança não degrade a proteção da dignidade humana. De fato, a proposta de pessoa eletrônica enfrentou resistência política e acadêmica: a Comissão Europeia acabou por não encampar essa recomendação do Parlamento. No *AI Act* em discussão na UE, optou-se por responsabilizar os sujeitos tradicionais (desenvolvedores, fornecedores, operadores) com base no risco da atividade, sem atribuir personalidade aos algoritmos.

A ideia de personalidade eletrônica, assim, foi momentaneamente afastada do projeto europeu, embora não esteja completamente sepultada no debate filosófico-jurídico. Autores minoritários ainda defendem que, futuramente, frente a IAs altamente avançadas, talvez seja necessária alguma forma de reconhecimento jurídico específico (KURKI, 2019, p. 143-165; SOLUM, 1992, p. 1231-1287).

Por ora, porém, o consenso regulatório caminha em sentido diverso: manter as IAs como objetos jurídicos, aperfeiçoando as regras existentes de imputação de responsabilidade aos seres humanos ligados a elas.

Em complemento aos modelos citados, discute-se também a utilização de mecanismos de seguro obrigatório e fundos de garantia para cobrir danos de IA. Tal ideia parte do pragmatismo de que, independentemente de culpa, haverá acidentes e prejuízos causados por sistemas inteligentes, de modo que espalhar o risco entre os envolvidos pode ser a solução mais eficiente.

Lopes ainda menciona a hipótese de exigir que fabricantes ou operadores de certas IAs contratem seguros de responsabilidade civil – medida similar à vigente para veículos automotores (seguro DPVAT) – garantindo indenização rápida às vítimas, sem travas quanto à determinação de culpa. Essa alternativa, embora não seja uma teoria de responsabilidade em si, integra o arsenal de ferramentas jurídicas da era digital para lidar com danos difusos e de origem tecnológica complexa.

Por fim, vale frisar os desafios na implementação dessas propostas de responsabilização na prática. Mesmo adotando-se a responsabilidade objetiva ou presumida, haverá questões espinhosas, como por exemplo: como definir o nexo causal em sistemas de IA opacos?; quem são exatamente os “operadores” responsáveis (o desenvolvedor do algoritmo, o fornecedor do software, o usuário final que o publica)?; como gradar os níveis de autonomia ou risco de um sistema de IA de forma juridicamente segura? – tema em que o próprio PL 2338/2023 recebeu críticas por certa falta de objetividade na definição do que seja alto risco e graus de autonomia.

Além disso, a rápida evolução tecnológica pode tornar regras muito estanques obsoletas em pouco tempo, demandando que a legislação seja flexível e principiológica o bastante para se adaptar a novas gerações de AI (por isso alguns

autores advogam por "*regulação responsiva*" e uso de sandboxes regulatórios no setor de IA).

Também será crucial investir em capacitação técnica do Judiciário e dos peritos, para que possam compreender o funcionamento dos algoritmos e aplicar corretamente conceitos como explicabilidade e avaliação de risco nos litígios concretos (BRAGA; PEREZ, 2025, p. 25-26).

Em suma, a responsabilidade civil na era digital demanda soluções inovadoras e colaborativas, repensando os conceitos clássicos sem romper com a segurança jurídica. Os caminhos em discussão – seja a objetivação da responsabilidade, a criação de normas específicas de risco, ou ainda a rejeitada ideia de pessoa eletrônica – revelam a busca por um equilíbrio: garantir que haja sempre um responsável solvente pelos danos causados pela IA (evitando lacunas de indenização), sem tolher o progresso tecnológico.

A era dos agentes não humanos impõe ao Direito a tarefa de ajustar suas lentes, ampliando as bases da responsabilidade civil de modo a englobar os novos fenômenos. Somente assim será possível assegurar que a Inteligência Artificial permaneça a serviço da humanidade – e não à margem da *accountability* jurídica – na construção de uma sociedade digital justa e segura.

CONCLUSÃO

Em síntese, este trabalho trouxe à luz que a rápida evolução dos *chatbots* baseados em Inteligência Artificial – hoje empregados em diversos setores para otimizar atendimento e processos – trouxe benefícios operacionais inegáveis, porém acompanhados de novos riscos jurídicos. Verificou-se que esses agentes conversacionais podem fornecer informações equívocas ou até fraudulentas, amplificando desinformações e preconceitos embutidos em seus dados de treinamento.

Essa constatação inicial evidenciou uma lacuna na lei: o ordenamento jurídico brasileiro ainda não oferece respostas plenamente eficazes para os danos causados por sistemas autônomos de conversação, dada a assimetria informacional e a dificuldade de enquadrar tecnicamente suas condutas nos modelos tradicionais de responsabilidade civil.

Por isso, o estudo partiu de um panorama técnico-evolutivo da IA e dos *chatbots* – seu funcionamento por *machine learning*, capacidade de processamento em linguagem natural e relativa autonomia decisória – para contextualizar os desafios legais emergentes na era digital.

Ao longo do trabalho, examinaram-se os fundamentos da responsabilidade civil no direito brasileiro, diferenciando a responsabilidade subjetiva (baseada em culpa ou dolo) da objetiva (calcada no risco da atividade). Esse arcabouço teórico foi crucial para analisar a aplicabilidade das normas vigentes aos casos de danos informacionais causados por *chatbots*.

Constatou-se que, embora o Código Civil e o Código de Defesa do Consumidor já prevejam hipóteses de responsabilidade objetiva – especialmente em atividades de risco ou nas relações de consumo –, tais ferramentas legais precisam ser reinterpretadas para abarcar os prejuízos decorrentes de agentes autônomos.

Evidenciou-se que insistir unicamente na prova de culpa do fornecedor é inadequado diante da opacidade algorítmica e da autonomia desses sistemas, que frequentemente impedem a identificação de um ato humano específico causador do dano. Assim, sugeriu-se que as empresas de tecnologia sejam responsabilizadas à luz da teoria do risco do empreendimento, protegendo as vítimas independentemente da prova de negligência individual.

Paralelamente, abordou-se a função social da reparação civil e os deveres informacionais dos fornecedores de IA destacando que a boa-fé objetiva e a tutela da confiança do consumidor impõem às empresas um padrão elevado de transparência e diligência. Em ambientes digitais marcados pela vulnerabilidade do usuário e pela assimetria de informação, não basta cumprir formalmente o dever de informar – é necessário garantir que as informações sobre o funcionamento, limitações e riscos dos *chatbots* sejam claras, acessíveis e verídicas, sob pena de violação dos direitos básicos do consumidor.

Também foi analisada a aplicação da Lei Geral de Proteção de Dados (LGPD) no contexto da IA, reconhecendo seus avanços e limites. Ficou claro que a LGPD, embora não concebida exclusivamente para IA, fornece princípios e obrigações relevantes que incidem sobre sistemas algorítmicos – como a necessidade de consentimento adequado, transparência no tratamento automatizado e segurança dos dados pessoais.

Em especial, ressaltou-se o direito conferido ao titular de revisar decisões automatizadas (art. 20 da LGPD) como um marco inicial de tutela contra decisões de *chatbots* ou algoritmos que afetem interesses individuais.

No entanto, o alcance restrito desse dispositivo (limitado a decisões inteiramente automatizadas) e as dificuldades práticas de enforcement mostram que a LGPD, isoladamente, não supre todas as lacunas frente à complexidade da IA generativa. Identificou-se a necessidade de fortalecer a governança algorítmica e a atuação da Autoridade Nacional de Proteção de Dados (ANPD) para fiscalizar de perto o uso ético e responsável de IA, bem como garantir efetividade aos direitos dos usuários (por exemplo, exigindo explicações inteligíveis sobre o funcionamento dos *chatbots* e intervenções humanas nos casos críticos).

A pesquisa mapeou ainda os diversos danos oriundos da desinformação algorítmica, mostrando que as respostas errôneas ou tendenciosas de um chatbot podem ocasionar tanto prejuízos patrimoniais (perdas financeiras, gastos indevidos) quanto danos extrapatrimoniais (ofensa à honra, discriminação, abalo moral). Foram apresentados exemplos concretos: desde erros em serviços automatizados que lesam economicamente consumidores, até fake news difundidas por algoritmos que maculam reputações ou propagam discurso de ódio. Inclusive, reconheceu-se que esses danos podem assumir dimensão coletiva ou difusa – como no caso de

desinformação em massa que abala a confiança social ou compromete processos democráticos –, o que desafia os mecanismos clássicos de reparação centrados em vítimas individualizadas.

A partir da análise de jurisprudência nacional e estrangeira, verificou-se uma tendência dos tribunais em adaptar os institutos tradicionais para coibir tais práticas lesivas: decisões brasileiras recentes já responsabilizam empresas por uso negligente de algoritmos (por exemplo, um caso de discriminação automatizada em recrutamento), aplicando princípios do CDC e do Código Civil para assegurar indenizações por danos morais e materiais.

No mesmo sentido, súmulas e precedentes do STJ têm presumido o dano moral em situações de cadastro negativo indevido ou dados incorretos – espécies de "fake news financeiras" – reconhecendo o dever de reparar pelo simples fato da informação falsa ter lesionado direitos de personalidade do consumidor.

Esse movimento jurisprudencial demonstra que a transformação digital não exime fornecedores, plataformas e desenvolvedores de seus deveres de cautela e lealdade: no ambiente virtual, persiste a responsabilidade civil pelos ilícitos, moldada agora às especificidades técnicas da IA.

Por fim, o estudo dedicou-se aos desafios regulatórios contemporâneos e às propostas de aprimoramento normativo e de governança tecnológica no Brasil. Identificou-se um consenso na literatura e nas políticas emergentes de que é urgente construir um marco regulatório específico para IA, apto a suprir as insuficiências das leis atuais. No cenário legislativo brasileiro, destaca-se o Projeto de Lei nº 2338/2023, que busca instituir um Marco Legal de IA inspirado no modelo de regulação por níveis de risco da União Europeia.

Essa iniciativa propõe requisitos proporcionais à criticidade de cada sistema de IA – impondo, por exemplo, rigorosos deveres de transparência, avaliação de risco, auditoria e supervisão humana para aplicações de "alto risco" (como algoritmos em saúde, finanças ou veículos autônomos), enquanto flexibiliza exigências para sistemas de baixo risco ou meramente auxiliares.

Caso aprovado, esse PL consolidará a opção por um regime de responsabilização objetivo no Brasil: os fornecedores e operadores de IA responderão integralmente pelos danos causados, independente de culpa, com inversão do ônus da prova a favor do lesado.

Essa abordagem, alinhada à lógica preventiva europeia, visa eliminar as “zonas de irresponsabilidade” associadas à autonomia algorítmica, garantindo que sempre haja um agente responsável e solvente pelos prejuízos advindos da tecnologia.

Outrossim, rechaçou-se, no momento, a ideia polêmica de atribuir personalidade jurídica aos sistemas de IA (as chamadas “pessoas eletrônicas”), entendendo que a solução mais prudente é manter os algoritmos como objetos jurídicos e aperfeiçoar as regras de imputação aos atores humanos que os desenvolvem, comercializam ou controlam.

Foram apontados mecanismos complementares, como a exigência de seguros obrigatórios ou fundos de compensação para cobrir danos de IA, também aparecem como medidas práticas para repartir os riscos e assegurar indenização célere às vítimas, sem paralisar a inovação.

Ademais, enfatizou-se a importância de fomentar a autorregulação responsável por parte das empresas de tecnologia – adotando códigos de ética, transparência algorítmica, auditorias independentes e programas internos de compliance em IA – em diálogo com as normas estatais. Esse modelo cooperativo de governança, aliando instrumentos legais vinculantes a iniciativas privadas de boas práticas, mostra-se adequado à realidade brasileira, pois equilibra o estímulo à inovação com a proteção dos direitos fundamentais. Não obstante, reconheceu-se que a operacionalização dessas propostas impõe desafios contínuos: será necessário definir com precisão os conceitos jurídicos de “risco elevado” e “operador de IA”, atualizar constantemente a legislação diante de novas gerações tecnológicas e capacitar tecnicamente o Judiciário e órgãos fiscalizadores para lidarem com questões complexas de algoritmos, explicabilidade e causalidade.

Conclui-se, portanto, que a responsabilidade civil na era da inteligência artificial demanda uma renovação paradigmática dos fundamentos jurídicos tradicionais. As contribuições do trabalho evidenciam a necessidade de normas específicas e complementares – como um marco legal da IA e ajustes no CDC e na LGPD – combinadas com uma postura proativa das empresas no aprimoramento de governança tecnológica e ética digital.

Somente com esse conjunto de medidas será possível mitigar a assimetria informacional entre usuários e fornecedores de IA e enfrentar o potencial lesivo dos algoritmos autônomos sem tolher o progresso tecnológico. Em outras palavras,

defende-se a construção de um modelo jurídico propositivo, que contemple tanto instrumentos estatais eficazes (regulação por risco, fiscalização pela ANPD e demais agências, sanções proporcionais) quanto mecanismos de autorregulação (transparência, *accountability* e boas práticas corporativas), tendo em vista a tutela dos direitos fundamentais dos cidadãos e a promoção de maior segurança jurídica nas relações digitais.

Através desse equilíbrio entre inovação e responsabilidade, estar-se-á assegurando que os *chatbots* e demais sistemas de IA permaneçam a serviço da humanidade – fornecendo benefícios à sociedade –, porém devidamente subordinados à *accountability* jurídica.

Dessa forma, o ordenamento jurídico brasileiro poderá responder de forma mais sólida e coerente aos desafios contemporâneos impostos pela inteligência artificial, prevenindo danos algorítmicos, reparando injustiças e fortalecendo a confiança dos usuários no ecossistema digital.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE LAWTECHS E LEGALTECHS (AB2L). *"Chatbots e responsabilidade civil"*. 14 jan. 2019. (Discussão de medidas para minimizar riscos jurídicos de *chatbots*).

ALMADA, Marco; MARANHÃO, Juliano. *Contribuições e limites da Lei Geral de Proteção de Dados para a regulação da inteligência artificial no Brasil. Revista de Direito Público*, Brasília, v. 20, n. 106, p. 385-413, abr./jun. 2023. DOI: 10.11117/rdp.v20i106.6957.

AMARAL, Julião Gonçalves. *A expansão da inteligência artificial e seu impacto nas dinâmicas sociais: desafios e responsabilidade*s. Revista da UFMG, v. 30, 2023.

AMORIM, Antônio Biasotti; SILVA, Rodrigo Cardoso. *Governança de IA no Brasil: proposta de modelo para equilíbrio tecnológico e econômico*. 2025.

BARBOSA, Vinícius de Oliveira Morais. *Inteligência artificial e advocacia privada: impactos, questões éticas e regulatórias sob a perspectiva da LGPD*. 2024.

BARROSO, Luís Roberto. *Inteligência artificial, plataformas digitais e democracia: direito e tecnologia no mundo atual*. Belo Horizonte: Fórum, 2024. 265 p. [1266776] SEN STJ.

BARROS, Raissa Dantas Teixeira de. *Direito informacional e Inteligência Artificial: uma análise do caso da coleta de dados pessoais feita pela Meta sob o viés do direito consumerista brasileiro.* 2024.

BIONI, Bruno; DIAS, Daniel. *Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor*. Civilistica. com, v. 9, n. 3, p. 1-23, 2020.

BRASIL. *Constituição da República Federativa do Brasil de 1988*. Brasília, DF: Senado Federal, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm.

BRASIL. *Código Civil. Lei nº 10.406, de 10 de janeiro de 2002*. Brasília, DF: Presidência da República, 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. *Dispõe sobre a proteção do consumidor e dá outras providências*. Brasília, DF: Diário Oficial da União, 1990.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. *Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet)*. Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018.

BRASIL. Superior Tribunal de Justiça. *Recurso Especial n. 1010322-67.2018.8.26.0152/SP*. Rel. Min. Maria Thereza de Assis Moura. Decisão monocrática, 2021. Disponível em: https://stj.jus.br. Acesso em: 7 out. 2025.

BRASIL. Superior Tribunal de Justiça. *Súmula n. 385 – Dano moral presumido por inscrição indevida*. Brasília, 2016. Disponível em: https://stj.jus.br. Acesso em: 7 out. 2025.

BRASIL. Tribunal de Justiça de Minas Gerais. *Agravo de Instrumento n. 1.0000.20.597631-9/001*. Rel. Des. Marcos Henrique Caldeira Brant. Julgado em 23 jun. 2021. Disponível em: https://tjmg.jus.br. Acesso em: 7 out. 2025.

BRASIL. Tribunal de Justiça de São Paulo. *Processo n. 1022312-33.2022.8.26.0114. Juíza Renata Oliva B. de Souza*. Sentença de 21 nov. 2022. Disponível em: https://tjsp.jus.br. Acesso em: 7 out. 2025.

BRASIL. Tribunal de Justiça do Maranhão. *Ação Civil Pública n. 0816292-73.2020.8.10.0001*. Juiz Douglas de Melo Martins. Sentença de 17 mar. 2023. Disponível em: https://tjma.jus.br. Acesso em: 7 out. 2025.

CAMPOS, Rodrigo. *Inteligência Artificial no Setor Jurídico: Exemplos de Inteligência Artificial Revolucionando o Setor Jurídico.* Blog Lexter, 31 out. 2024. Disponível em: https://blog.lexter.ai/inteligencia-artificial-setor-juridico. Acesso em: 23 jul. 2025.

CANADA. Jake Moffatt v. Air Canada. 2024 BCCRT 149. Civil Resolution Tribunal, decisão de 14 fev. 2024. Disponível em: https://www.canlii.org/en/bc/bccrt/doc/2024/2024bccrt149. Acesso em: 7 out. 2025.

CASEIRO, Sofia. *O impacto da inteligência artificial na democracia*. In: IV Congresso Internacional de Direitos Humanos de Coimbra: Anais, 2019.

CIMARELLI, Larissa Velloso. *A Vulnerabilidade Do Consumidor Nas Relações De Consumo Mediadas Por Inteligência Artificial.* Revista Foco (Interdisciplinary Studies Journal) 18.6 (2025).

COELHO, Fábio Ulhoa. *Curso de direito civil, volume 2: obrigações : responsabilidade civil* – 5. ed. – São Paulo: Saraiva, 2012.

CORREIA, Atalá. *O dever de informar nas relações de consumo.* Revista da Escola da Magistratura do Distrito Federal, Brasília, n. 13, p. 79-96, 2011.

DA COSTA OLIVEIRA, Carolina. *Desinformação E Responsabilidade Civil*. 2024. Tese de Doutorado. Universidade de Coimbra.

DAS NEVES BRAGA, Pedro Alonso; PEREZ FILHO, Augusto Martinez. *Regulamentação Da Inteligência Artificial No Poder Judiciário: Perspectivas, Desafios E O Diálogo Entre O Marco Europeu E As Iniciativas Brasileiras*. Revista Contemporânea, v. 5, n. 7, p. e8570-e8570, 2025.

DE FARIA, Pedro Alberto Schiller. *A Responsabilidade Civil na Inteligência Artificial*. 2022. Tese de Doutorado. PUC-Rio.

DE SANTANNA, Mayara Bartaquini. *O Impacto da Inteligência Artificial na Aplicabilidade da Transparência e Proceedings on Privacy Enhancing Technologies*, v. 4, p. 484-499, 2023.

DE SOUZA LIMA, Carlos et al. *O Paradoxo Da Soberania Digital: Uma Análise Filosófica Sobre A Governança Algorítmica, Direitos Humanos E Autonomia Na Era Da Vigilância*. Magno Medeiros Elen Cristina Geraldes Janara Sousa Marcelo Fonseca Santos, p. 106, 2025.

DINIZ, Maria Helena. *Código Civil comentado: doutrina e jurisprudência.* 16. ed. São Paulo: Saraiva, 2010.

DINIZ, Maria Helena. *Curso de direito civil brasileiro, volume I: teoria geral do direito civil* - 31. ed. São Paulo: Saraiva, 2019.

DINIZ, Maria Helena. *Curso de Direito Civil Brasileiro – Vol. 7: Responsabilidade Civil*. 30. ed. São Paulo: Saraiva, 2010.

DOS SANTOS NETO, João Leonardo; CORREA, Jonas Sousa. *Riscos De Um Futuro A Base Da Inteligência Artificial. Uma Visão Abrangente Da Computação*, p. 26.

IEG – Institute of Executive Education. Aproximadamente 50% dos CSCs brasileiros utilizam chatbot. Blog IEG, 2024. Disponível em: https://ieg.com.br/blog/aproximadamente-50-dos-cscs-brasileiros-utilizam-chatbot/. Acesso em: 23 jul. 2025.

GAGLIANO, Pablo Stolze; PAMPLONA FILHO, Rodolfo. *Manual de direito civil – volume único.* 4ª ed. rev. ampl. e atual. São Paulo: Saraiva Educação, 2020.

GAGLIANO, Pablo Stolze; PAMPLONA FILHO, Rodolfo. *Novo Curso de Direito Civil: Responsabilidade Civil*. 6. ed. São Paulo: Saraiva, 2017.

GAMBA, Sérgio Roberto Horst. *Responsabilidade e transparência algorítmica na inteligência artificial*. Revista Ibmec de Ciência, Tecnologia e Inovação (RISTI), Brasília, 2023.

GONÇALVES, Carlos Roberto. *Direito Civil Brasileiro – Vol. IV: Responsabilidade Civil*. 18. ed. São Paulo: Saraiva, 2018.

GUTIERREZ, Carlos. *Regulação da Inteligência Artificial: Comentários ao PL 5051/2019***.** In: Calamidade Pública: repensando o direito em tempos de crise. Porto Alegre: Editora E-Publicar, 2020.

INSTITUTO FEDERAL DE SANTA CATARINA – IFSC. Quais os impactos do ChatGPT e da Inteligência Artificial na Educação? IFSC Verifica, 28 fev. 2023 (atualizado em 1 mar. 2023). Disponível em: https://www.ifsc.edu.br/web/ifsc-verifica/w/quais-os-impactos-do-chatgpt-e-da-inteligencia-artificial-na-educacao/. Acesso em: 23 jul. 2025.

JETCHAT. *Chatbots na Educação: Transformando a Aprendizagem com Inteligência Artificial*. Blog JetChat, 1 abr. 2025. Disponível em: https://jetchat.com.br/inteligencia-artificial/chatbots-na-educacao-transformando-aprendizagem-jetchat/. Acesso em: 23 jul. 2025.

KRETZMANN, Renata Pozzi. *O dever de informar do fornecedor e a eficácia jurídica da informação nas relações de consumo: precisões conceituais*. Dissertação

(Mestrado em Direito) – Universidade Federal do Rio Grande do Sul, Porto Alegre, 2018.

LIMA, Maycon Rodrigues de Souza. *Análise comparativa da Lei Geral de Proteção de Dados (LGPD) e do Regulamento Geral de Proteção de Dados (GDPR): Impactos na Regulação da Inteligência Artificial e na proteção da Privacidade do usuário*. 2024.

LOPES, Giovana Figueiredo Peluso et al. *Inteligência artificial (IA): considerações sobre personalidade, imputação e responsabilidade*. 2020.

LUNARDI, Henrique Lapa. *Inteligência artificial, direitos humanos e o consumo: análise da vulnerabilidade da autonomia do consumidor e as novas tecnologias,* 2022.

MACEDO, Suélem Viana; MENDES, Mikaelly Gonçalves. *Lei Geral de Proteção de Dados: Respeito À Privacidade E À Responsabilidade Civil Dos Agentes De Tratamento De Dados Pessoais No Brasil*. Revista Científica UNIFAGOC-Jurídica, v. 9, n. 2, 2024.

MATIAS, Edinalda de Araújo; ARAÚJO, José Henrique Mouta. *Inteligência Artificial e o Direito: novas tendências e desafios.* Revista XYZ, v.10, n.2, 2021. (Trechos comparando aprendizado de máquina ao humano).

MANZATO, Welington Junior Jorge; SOARES, Marcelo Negri; CUGULA, Jarbas Rodrigues Gomes. *Direitos da personalidade e IA: segurança jurídica na automação contratual*. Derecho y Cambio Social, v. 22, n. 80, p. 1-20, 2025.

MARQUES, Claudia Lima. *Contratos no Código de Defesa do Consumidor: o novo regime das relações contratuais*. 7. ed. São Paulo: Revista dos Tribunais, 2014.

MENDES, Angela Maria de Aguiar et al. *Inteligência artificial: uma análise sob a ótica da responsabilidade civil.* Revista Brasileira de Direito e Novas Tecnologias, Vitória, v. 12, n. 2, p. 72-91, 2025.

MORAIS JÚNIOR, Ricardo Antonio Maia de. *Accountability e direito fundamental à proteção de dados pessoais enquanto limites ao uso da inteligência artificial na relação de emprego*. Dissertação (Mestrado em Direito) – Universidade Federal do Ceará, Fortaleza, 2023.

MORETTI, Juliano Lazzarini; ZUFFO, Milena Maltese. *LGPD e inteligência artificial: Um estudo comparado*. Revista de Direito Internacional e Globalização Econômica, v. 13, n. 13, p. 21-42, 2025.

NARDI, Luize Gaggiola. *Uma perspectiva analítica da aplicação da inteligência artificial (IA) à Lei Geral de Proteção de Dados Pessoais (LGPD)*. 2023.

PAÍSES BAIXOS. *NJCM et al. v. Netherlands (SyRI)*. Rechtbank Den Haag, vonnis de 5 fev. 2020, zaak nr. C/09/550982. Disponível em: https://uitspraken.rechtspraak.nl/#!/details?id=ECLI:NL:RBDHA:2020:865. Acesso em: 7 out. 2025

PASQUALE, Frank. *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge: Harvard University Press, 2015.

PEREIRA, Kieza Inglid Chefer; DE LEMOS DIAS, Taciana; GIANORDOLI, Victor. *Entre Normas Genéricas E Necessidades Específicas: A Regulamentação Da Inteligência Artificial No Brasil.* Derecho y Cambio Social, v. 22, n. 80, p. e128-e128, 2025.

PESSOA, Vanessa Gabriele Lima et al. *Princípios Éticos na IA: O Impacto da Governança Ética na Redução de Vieses*. 2024.

RATTI, Helena Soares. *Responsabilidade civil perante erros causados por sistemas de inteligência artificial*. 2024.

REVISTA FT. *Aplicação de chatbots para automatização do atendimento acadêmico: um estudo de caso*. Revista FT, [s.d.]. Disponível em: https://revistaft.com.br/aplicacao-de-chatbots-para-automatizacao-do-atendimento-academico-um-estudo-de-caso/. Acesso em: 23 jul. 2025.

ROCHA, Amélia Soares da; TORRES, Ismael Braz. *O direito do consumidor e as novas tecnologias: Sistema Nacional de Informações de Defesa do Consumidor – SINDEC*. *Revista de Direito do Consumidor*, São Paulo, v. 32, n. 4, p. 145-166, 2020.

SANTANNA, Mayara Bartaquini de. *O impacto da inteligência artificial na aplicabilidade da transparência e anonimização na proteção de dados*. Dissertação (Mestrado em Direito Político e Econômico) – Universidade Presbiteriana Mackenzie, São Paulo, 2023.

SANTOS, Jheinifer Machado dos. *Inteligência artificial: considerações sobre o racismo algorítmico e o cenário da responsabilidade civil no Brasil*. 2024.

SARLET, Ingo Wolfgang; SAAVEDRA, Giovani Agostini. *Fundamentos jusfilosóficos e âmbito de proteção do direito fundamental à proteção de dados pessoais*. Revista Direito Público, 2020.

SARLET, Ingo Wolfgang. *Proteção de dados pessoais como direito fundamental na constituição federal brasileira de 1988. Direitos Fundamentais & Justiça*, 2020.

SARLET, Ingo Wolfgang. *Proteção de dados pessoais como direito fundamental autônomo na Constituição Brasileira de 1988. Direitos fundamentais na perspectiva da democracia interamericana*, 2021.

SILVA, Gabriela Buarque Pereira et al. *Responsabilidade civil, riscos e inovação tecnológica: os desafios impostos pela inteligência artificial*. 2021.

SILVA, Hellen Eduarda Rodrigues et al. *RESPONSABILIDADE CIVIL NA ERA DIGITAL: Desafios E Perspectivas*. Revista Acadêmica Online, v. 10, n. 50, p. 1-18, 2024.

SISTI, LUCAS FELIPE, and FRANC. I. S. C. O. BELTRÃO–PR. *A Injuridicidade Em Algoritmos De Inteligência Artificial*.

SOUZA, Marcela Cristina de. *RESPONSABILIDADE CIVIL NO TRATAMENTO DE DADOS: Impactos da Inteligência Artificial na Proteção de Informações Pessoais*. 2025.

TÂNGARI, Guillermo. *42,4% das 500 maiores instituições de ensino do Brasil usam chatbots*. Blog Mkt4Edu, 10 mar. 2020 (atualizado em 19 jan. 2024). Disponível em: https://www.mkt4edu.com/blog/apenas-424-das-500-maiores-instituicoes-de-ensino-do-brasil-usam-chatbots-revela-estudo/. Acesso em: 23 jul. 2025.

TARTUCE, Flávio. *Manual de direito civil: volume único.* 7ª ed. rev., atual. e ampl. Rio de Janeiro: Forense; São Paulo: MÉTODO, 2017.

TASSO, Fernando Antonio. *A responsabilidade civil na Lei Geral de Proteção de Dados e sua interface com o Código Civil e o Código de Defesa do Consumidor.* Cadernos Jurídicos, São Paulo, ano, v. 21, p. 97-115, 2020.

UNITED STATES. *Mark Walters v. OpenAI LLC, Case No. 23-A-04860-2*. Superior Court of Gwinnett County (Georgia). Order of May 19, 2025. Disponível em: https://www.gwinnettcourts.com. Acesso em: 7 out. 2025.

UNITED STATES. *Megan Garcia v. Character Technologies Inc. U.S. District Court, M.D*. Florida, 2025 (em andamento). Disponível em: https://pacer.uscourts.gov. Acesso em: 7 out. 2025.

VELLOSO, Larissa Cimarelli. *A VULNERABILIDADE DO CONSUMIDOR NAS RELAÇÕES DE CONSUMO MEDIADAS POR INTELIGÊNCIA ARTIFICIAL*. REVISTA FOCO, v. 18, n. 6, p. e8723-e8723, 2025.

VENOSA, Sílvio de Salvo. *Direito Civil – Responsabilidade Civil*. 15. ed. São Paulo: Atlas, 2017.

Verbicaro, Dennis, Janaina Vieira Homci, and Gisele Santos Fernandes Goes. *A Aplicação Da Inteligência Artificial Nos Tribunais Brasileiros: Um Estudo A Partir Da Perspectiva Da Vulnerabilidade Algorítmica Do Consumidor.*

VETTORAZZI, Karlo Messa; BOTTINI, Julia de Mello. *Vulnerabilidade digital e o dever de informação nas relações de consumo*. Revista PPC – Políticas Públicas e Cidades, Curitiba, v. 14, n. 3, p. 1-9, 2025. DOI: https://doi.org/10.23900/2359-1552v14n3-56-2025.

ZUBOFF, Shoshana. *A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder*. Tradução de Ilana Goldfeld. 1. ed. Rio de Janeiro: Intrínseca, 2021. ISBN 978-65-5560-145-9.