

# **II ENCONTRO NACIONAL DE DIREITO DO FUTURO - II ENDIF**

**PROCESSO E TECNOLOGIA**

---

P963

Processo e tecnologia [Recurso eletrônico on-line] organização II Encontro Nacional de Direito do Futuro: Escola Superior Dom Helder Câmara – Belo Horizonte;

Coordenadores: Vinícius Lott Thibau, Helen Cristina de Almeida Silva e Magno Federici Gomes – Belo Horizonte: Escola Superior Dom Helder Câmara - ESDHC, 2025.

Inclui bibliografia

ISBN: 978-65-5274-415-9

Modo de acesso: [www.conpedi.org.br](http://www.conpedi.org.br) em publicações

Tema: Justiça social e tecnológica em tempos de incerteza.

1. Direito do Futuro. 2. Justiça Social. 3. Justiça Tecnológica. I. II Encontro Nacional de Direito do Futuro (1:2025 : Belo Horizonte, MG).

CDU: 34

---

## **II ENCONTRO NACIONAL DE DIREITO DO FUTURO - II ENDIF**

### **PROCESSO E TECNOLOGIA**

---

#### **Apresentação**

O II Encontro Nacional de Direito do Futuro (II ENDIF), organizado pelo Centro Universitário Dom Helder com apoio técnico do Conselho Nacional de Pesquisa e Pós-graduação em Direito – CONPEDI, reafirma-se como um espaço qualificado de produção, diálogo e circulação do conhecimento jurídico, reunindo a comunidade científica em torno de um propósito comum: pensar, com rigor metodológico e sensibilidade social, os caminhos do Direito diante das transformações que marcam o nosso tempo. Realizado nos dias 09 e 10 de outubro de 2025, em formato integralmente on-line, o evento assumiu como tema geral “Justiça social e tecnológica em tempos de incerteza”, convidando pesquisadoras e pesquisadores a enfrentar criticamente os impactos da inovação tecnológica, das novas dinâmicas sociais e das incertezas globais sobre as instituições jurídicas e os direitos fundamentais.

Nesta segunda edição, os números evidenciam a força do projeto acadêmico: 408 trabalhos submetidos, com a participação de 551 pesquisadoras e pesquisadores, provenientes de 21 Estados da Federação, culminando na organização de 31 e-books, que ora se apresentam à comunidade científica. Essa coletânea traduz, em linguagem acadêmica e compromisso público, a vitalidade de uma pesquisa jurídica que não se limita a descrever problemas, mas busca compreendê-los, explicar suas causas e projetar soluções coerentes com a Constituição, com os direitos humanos e com os desafios contemporâneos.

A publicação dos 31 e-books materializa um processo coletivo que articula pluralidade temática, densidade teórica e seriedade científica. Os textos que compõem a coletânea passaram por avaliação acadêmica orientada por critérios de qualidade e imparcialidade, com destaque para o método double blind peer review, que viabiliza a análise inominada dos trabalhos e exige o exame por, no mínimo, dois avaliadores, reduzindo subjetividades e preferências ideológicas. Essa opção metodológica é, ao mesmo tempo, um gesto de respeito à ciência e uma afirmação de que a pesquisa jurídica deve ser construída com transparência, responsabilidade e abertura ao escrutínio crítico.

O II ENDIF também se insere em uma trajetória institucional já consolidada: a primeira edição, realizada em junho de 2024, reuniu centenas de pesquisadoras e pesquisadores e resultou na publicação de uma coletânea expressiva, demonstrando que o Encontro se consolidou, desde o início, como um dos maiores eventos científicos jurídicos do país. A

continuidade do projeto, agora ampliada em escopo e capilaridade, reafirma a importância de se fortalecer ambientes acadêmicos capazes de integrar graduação e pós-graduação, formar novas gerações de pesquisadoras e pesquisadores e promover uma cultura jurídica comprometida com a realidade social.

A programação científica do evento, organizada em painéis temáticos pela manhã e Grupos de Trabalho no período da tarde, foi concebida para equilibrar reflexão teórica, debate público e socialização de pesquisas. Nos painéis, temas como inteligência artificial e direitos fundamentais, proteção ambiental no sistema interamericano, proteção de dados e herança digital foram tratados por especialistas convidados, em debates que ampliam repertórios e conectam a produção acadêmica aos dilemas concretos vividos pela sociedade.

A programação científica do II ENDIF foi estruturada em dois dias, 09 e 10 de outubro de 2025, combinando, no período da manhã, painéis temáticos com exposições de especialistas e debates, e, no período da tarde, sessões dos Grupos de Trabalho. No dia 09/10 (quinta-feira), após a abertura, às 09h, realizou-se o Painel I, dedicado aos desafios da atuação processual diante da inteligência artificial (“Inteligencia artificial y desafios de derechos fundamentales en el marco de la actuación procesal”), com exposição de Andrea Alarcón Peña (Colômbia) e debate conduzido por Caio Augusto Souza Lara. Em seguida, às 11h, ocorreu o Painel II, voltado à proteção ambiental no Sistema Interamericano, abordando a evolução da OC-23 ao novo marco da OC-32, com participação de Soledad Garcia Munoz (Espanha) e Valter Moura do Carmo como palestrantes, sob coordenação de Ricardo Stanziola Vieira. No período da tarde, das 14h às 17h, desenvolveram-se as atividades dos Grupos de Trabalho, em ambiente virtual, com apresentação e discussão das pesquisas aprovadas.

No dia 10/10 (sexta-feira), a programação manteve a organização: às 09h, foi realizado o Painel III, sobre LGPD e a importância da proteção de dados na sociedade de vigilância, com exposições de Laís Furuya e Júlia Mesquita e debate conduzido por Yuri Nathan da Costa Lannes; às 11h, ocorreu o Painel IV, dedicado ao tema da herança digital e à figura do inventariante digital, com apresentação de Felipe Assis Nakamoto e debate sob responsabilidade de Tais Mallmann Ramos. Encerrando o evento, novamente no turno da tarde, das 14h às 17h, seguiram-se as sessões dos Grupos de Trabalho on-line, consolidando o espaço de socialização, crítica acadêmica e amadurecimento das investigações apresentadas.

Ao tornar públicos estes 31 e-books, o II ENDIF reafirma uma convicção essencial: não há futuro democrático para o Direito sem pesquisa científica, sem debate qualificado e sem compromisso com a verdade metodológica. Em tempos de incerteza — tecnológica, social,

ambiental e institucional —, a pesquisa jurídica cumpre um papel civilizatório: ilumina problemas invisibilizados, questiona estruturas naturalizadas, qualifica políticas públicas, tensiona o poder com argumentos e oferece horizontes normativos mais justos.

Registramos, por fim, nosso reconhecimento a todas e todos que tornaram possível esta obra coletiva — autores, avaliadores, coordenadores de Grupos de Trabalho, debatedores e equipe organizadora —, bem como às instituições e redes acadêmicas que fortalecem o ecossistema da pesquisa em Direito. Que a leitura desta coletânea seja, ao mesmo tempo, um encontro com o que há de mais vivo na produção científica contemporânea e um convite a seguir construindo, com coragem intelectual e responsabilidade pública, um Direito à altura do nosso tempo.

Belo Horizonte-MG, 16 de dezembro de 2025.

Prof. Dr. Paulo Umberto Stumpf – Reitor do Centro Universitário Dom Helder

Prof. Dr. Francilm Jorge Sobral de Brito – Vice-Reitor e Pró-Reitor de Graduação do Centro Universitário Dom Helder

Prof. Dr. Caio Augusto Souza Lara – Pró-Reitor de Pesquisa do Centro Universitário Dom Helder

# **A RESPONSABILIDADE CIVIL DO FORNECEDOR PELO MAU USO DA INTELIGÊNCIA ARTIFICIAL: O CONTRASTE ENTRE A STRICT LIABILITY DA UNIÃO EUROPEIA E A LACUNA LEGISLATIVA BRASILEIRA**

## **SUPPLIER'S CIVIL LIABILITY FOR THE MISUSE OF ARTIFICIAL INTELLIGENCE: A COMPARATIVE ANALYSIS OF THE EUROPEAN UNION'S STRICT LIABILITY FRAMEWORK AND THE BRAZILIAN LEGISLATIVE GAP**

**Davi Santos Ribeiro <sup>1</sup>**  
**Gustavo Faria de Freitas <sup>2</sup>**

### **Resumo**

O objetivo do presente trabalho de pesquisa é apontar, no advento da era tecnológica e do uso contínuo da Inteligência Artificial (IA), as hipóteses de utilização maliciosa por um usuário final da inteligência e auferir, com isso, o responsável por indenizar civilmente pelo dano. Para isso, traz-se a previsão apresentada pela União Europeia da “strict liability” que imprescinde sutis ajustes para sanar as lacunas normativas e possibilitar a inserção no sistema jurídico brasileiro e, apenas dessa forma, é possível definir o campo da responsabilidade do fornecedor e os seus limites, sobretudo na hermenêutica da culpa e na descaracterização da omissão.

**Palavras-chave:** Responsabilidade civil, Inteligência artificial, Fornecedor

### **Abstract/Resumen/Résumé**

The purpose of this research is to examine, in the context of the technological era and the growing use of Artificial Intelligence (AI), the potential malicious use by end users and to determine who bears civil liability for resulting damages. To this end, the study considers the European Union's strict liability framework, which requires subtle adjustments to address normative gaps and enable integration into the Brazilian legal system. Only then is it possible to delineate the scope and limits of supplier liability, particularly regarding fault interpretation and the recharacterization of omission.

**Keywords/Palabras-claves/Mots-clés:** Civil liability, Artificial intelligence, Supplier

---

<sup>1</sup> Bacharel em Direito pela Universidade Federal de Viçosa, com endereço de e-mail: ribeirosdavi@gmail.com

<sup>2</sup> Graduando em Direito, na modalidade convencional, pela Escola Superior Dom Helder Câmara, com endereço de e-mail: gustavofreitas.0313@gmail.com

## 1 O advento da Inteligência Artificial e seus elementos inovativos

O avanço da tecnologia historicamente moldou novos contornos da sociedade e impactou na maneira com que os fenômenos jurídicos são interpretados. Na contemporaneidade, a difusão acelerada de sistemas de Inteligência Artificial (IA) inaugura um novo capítulo de questionamentos para a ciência jurídica, sobretudo no campo da responsabilidade civil.

A IA pode ser compreendida, em termos gerais, como um conjunto de técnicas computacionais concebidas para realizar tarefas que, se executadas por um ser humano, demandariam algum nível capacidade cognitiva<sup>1</sup>. A referida definição abarca uma vasta modalidade de tecnologias, sendo possível ainda aprofundar na classificação dos tipos de IA com relação à distinção das técnicas de funcionamento.

Para o estudo dos impactos da IA na responsabilidade civil é relevante compreender a separação entre os sistemas cujo comportamento, em razão da programação empregada, é determinístico, dentre aqueles que, por sua natureza e objetivo intrínseco, será probabilístico e não inteiramente previsível<sup>2</sup>.

A primeira vertente, também chamada de IA Simbólica ou IA Clássica, opera explicitamente baseadas em regras fixas, definidas mediante *scripts* lógicos e instruções de correlacionais. Assim, a partir da entrada de um dado, é percorrido um caminho lógico que é inteiramente previsível e auditável, de modo que para uma mesma informação o sistema produzirá invariavelmente o mesmo resultado.

Já no segundo cenário, tem-se a IA Conexionista, cuja principal característica é o Aprendizado de Máquina (Machine Learning) e Aprendizado Profundo (Deep Learning). Ao contrário de uma programação com regras explícitas e restritas, os modelos são treinados com vastos conjuntos de dados, a partir dos quais aprendem a reconhecer padrões e a fazer inferências de forma autônoma, apresentando respostas probabilísticas. Isso significa que, ainda que receba entradas de dados idênticos, o sistema pode apresentar respostas diversas.

Nota-se, portanto, que a IA simbólica permite delimitar com clareza a origem de um resultado lesivo: o resultado equivocado ocorreu ou pela inserção de um dado errado (falha do usuário) ou pela falha na regra programada para a respectiva tratativa (falha do programador).

---

<sup>1</sup> RUSSELL, Stuart J.; NORVIG, Peter. Artificial Intelligence: A Modern Approach. 4. ed. Upper Saddle River: Prentice Hall, 2020.

<sup>2</sup> VAINZOF, Rony; GUTIERREZ, Andriei Guerrero (coord.). Inteligência artificial: sociedade, economia e Estado. São Paulo: Thomson Reuters Brasil, 2021

De outro lado, a imprevisibilidade intrínseca aos modelos de IA Conexionista é um desafio aos parâmetros tradicionais da responsabilidade civil<sup>3</sup>. Os modelos de IA generativa, baseados em *Large Language Model* (LLM), que se enquadram nessa segunda classificação, foram difundidos e popularizados em larga escala por diversos setores e plataformas, contudo se encontram desacompanhados de uma atualização legislativa sobre o tema.

Com a popularização do acesso às ferramentas baseadas em IAs probabilísticas, já se identifica a utilização, por usuários, para fins indevidos ao inicialmente previstos pelo desenvolvedor, com potencial ocorrência de danos tanto aos próprios envolvidos quanto a terceiros e é nesse contexto que surge a questão central que orienta o presente trabalho: em que medida o ordenamento jurídico brasileiro está preparado para lidar com danos decorrentes do mau uso da inteligência artificial?

Diante da multiplicidade de agentes envolvidos, programador, fornecedor e usuário, bem como a imprevisibilidade da própria IA, há o rompimento do liame causal em quais situações? Na hipótese de o dano ter sido causado de forma exclusiva e diretamente pelo próprio sistema de IA, o critério para responsabilização do fornecedor envolvido na cadeia seria subjetivo ou objetivo? Admite-se alguma hipótese tradicional de excludente de ilicitude?

A resposta a estas indagações exige não apenas a análise das lacunas normativas nacionais, mas também a investigação das soluções propostas em outros ordenamentos, como a União Europeia, que adota a lógica da *strict liability* como forma de proteção efetiva dos lesados.

## **2 A modernização da hermenêutica da culpa civil e a responsabilização pela União Europeia do Fornecedor pelo mau uso da IA**

Imperativo destacar, desde já que, nas concepções ordenamentais brasileiras, não basta o cometimento de um ato ilícito para restar caracterizado o dever de reparação, é necessário que se perceba em cada caso concreto a existência de dano - patrimonial ou extrapatrimonial - e outros elementos que, inclusive, são hábeis a atrair o antedito dever de reparação para alguém que sequer foi o causador imediato do dano, como na responsabilidade objetiva do fornecedor prevista no Código de Defesa do Consumidor (CDC) ou nos casos previsto no CC como sendo o risco atrelado à atividade. Nesse sentido, diz-se que, à luz dos dispositivos normativos domésticos, via de regra nascerá o dever de indenizar da ação, seja ela comissiva ou omissiva,

---

<sup>3</sup> TEPEDINO, Gustavo; SILVA, Rodrigo da Guia (Coord.). O Direito Civil na era da Inteligência Artificial. São Paulo: Thomson Reuters Brasil/Revista dos Tribunais, 2020.

de um sujeito que, através de um ato ilícito, causa dano a outrem, de modo doloso ou ainda com culpa - em sentido distinto do Direito Penal e que será mais bem exposto aqui - e com incontestável nexos de causalidade entre a ação e o dano.

Para definirmos as primeiras linhas de pensamento, temos que entender que a instituição da culpa, em sua hermenêutica cível, não trata de uma questão pura e subjetiva de vontade do legislador de criar parâmetros da responsabilidade, mas sim do rompimento de um paradigma da era medieval que a mantinha interconectada com uma presunção penal de tal forma que, em função de sua natureza, não abrangia as intenções, o que acabava por inviabilizar a proteção da boa-fé nas relações pessoais. É justamente isso que diz o jurista brasileiro Anderson Schreiber.

Daí a necessidade de construção de um sistema de responsabilidade moderno, puramente civil, desvinculado da tradição medieval, e fundado não na violação de normas penais expressas, mas no legítimo exercício da liberdade individual, identificado, desde logo, e de forma exclusiva, com a noção de culpa. (Schreiber, 2015, p.13)

De igual forma, para se pensar as relações humanas em um Estado Democrático de Direito nos dizemos e presumimos livres para tomarmos as nossas próprias decisões, seja por uma concepção política-mercantil de liberalismo, seja por um ideal jurídico da liberdade de expressão, por questões bíblicas do livre arbítrio, ou outras mais correntes. Entretanto, num viés protecionista dos direitos pessoais, há de se admitir, como bem pontua Hans Hattenhauer, que a liberdade individual, em algum momento, possibilitará ao sujeito se valer de alguma torpeza para se beneficiar sobre alguém - ao exemplo tratado no presente instrumento textual do usuário final de uma IA que gera um código para software malicioso que vai atingir os dados de uma pessoa física ou confundir o sistema e simular contratos com instituições privadas - e, portanto, precisamos de algum mecanismo de responsabilização do indivíduo.

El hombre puede decidir libremente de qué modo desea alterar su entorno, pero, como el acto es libertad hecha realidad, hay que responder de él, y esta responsabilidad culmina en el deber de evitar por completo las consecuencias dañosas de un inadecuado uso de la libertad. (Hattenhauer, 1987, p.101)<sup>4</sup>

Dessa forma, em que pese a mudança de paradigma apontada, essa não estabelece um conceito para a culpa dentro das relações cíveis visando de fato a subjetividade das intenções, mas sim a criação de um parâmetro do conhecimento esperado para o homem médio na área e

---

<sup>4</sup> O homem pode decidir livremente de que modo deseja alterar o seu entorno, mas, como a ação é a liberdade feita realidade, deverá responder por ela, e esta responsabilidade culmina no dever de evitar por completo as consequências danosas de um uso inadequado da liberdade. (Tradução livre nossa)

como ele pode evitar as consequências de sua ação e é aí que emerge o primeiro problema da responsabilização do fornecedor pelo meu uso da Inteligência Artificial, até qual ponto o “*Machine Learning*” atua como um mecanismo de opacidade da previsão da “criatividade” do *script* e extrapola o conhecimento esperado para o programador, Fornecedor.

O desenvolvimento de uma rede neuro-computacional independente, notadamente nas IAs generativas – que criam códigos e *scripts* –, nascem não de um código estrito e limitado que padroniza as respostas do robô, mas sim de uma *Large Language Model* (LLM) que é, por uma brilhante explicação de Stryker (2025), uma categoria do *deep learning* que consiste em um modelo treinado sob uma vasta quantia de dados que geram, assim, uma linguagem neutra que se autotransforma através de padrões de texto informados para ampliar o alcance de sua capacidade. Nesse viés, entende-se que a linguagem-base da IA é dotada de um caráter expansionista e que se autorregula pelo *Machine Learning*, assim, ainda que seja possível o estabelecimento de certas travas na rede neural, essas se submeterão a preceitos e condições específicas do bloqueio que podem ser, talvez não tão facilmente mesmo que inegavelmente, superadas e “enganadas” pelo Consumidor final – sobretudo quando do entendimento que o termo “código”, para a programação, gera uma amplitude tal que não necessariamente será aplicada em um *software* malicioso.

É nítido portanto, que diferentemente do que prega o CDC e o CC brasileiros quando tratam os riscos atrelados à atividade do desenvolvedor, a capacidade expansionista e de autodesenvolvimento de uma Inteligência Artificial faz com que inexista uma responsabilidade objetiva que se frutifica em uma presunção absoluta de uso em prejuízo de outrem, vez que temos um bloqueio – chamado pelos autores americanos de *Opacity* – na presunção regular da conduta do robô, ou seja, quando o desenvolvedor cria uma IA generativa, presume-se que o código requerido pelo Consumidor final seja de fato utilizado de uma forma benéfica, posto que ele sempre será possível dessa forma.

While unpredicted behaviour in new situations nobody had ever thought about may also occur with software of a traditional kind, algorithms created with the help of machine learning cannot easily be analysed, in particular not when sophisticated methods of deep learning have been used. This ‘opacity’ of the code (‘black box effect’) means that it is not easy to explain why the AI behaved in a particular manner in a given situation, and even less easy to trace that behaviour back to any feature which could be called ‘defect’ of the code or to any shortcoming in the development process. (Wenderhost, 2020)<sup>5</sup>

---

<sup>5</sup> Enquanto comportamentos imprevisíveis, em novas situações as quais ninguém ainda pensou, também possam ocorrer com *softwares* mais tradicionais, algoritmos criados com a ajuda do *machine learning* não podem ser facilmente analisados, especialmente quando métodos mais sofisticados de *deep learning* - aprendizado

Vale dizer, também, que a não incidência do dever de indenizar sobre o Fornecedor, ante à ausência de sua culpa na má-utilização do sistema, não transfere de modo automático, “*in re ipsa*”, a responsabilidade ao Consumidor final, e foi no ímpeto de sanar a problemática suscitada que a União Europeia criou uma proposta de Ato Regulador, chamado *UE AI Act*, que traz algumas ideias sobre a ocorrência desses casos.

A bem da verdade, a instituição da “*strict liability*” foi criada tratar uma responsabilidade em casos que não se percebe o mau desenvolvimento da IA, isto é, não houve uma falha de fato no software – que desenvolveu algo lícito, ainda que não usado dessa forma – e nos casos em que não se visualiza uma política de vazamento de dados, chamado *non-compliance*.

Com isso, impera dizer que a União Europeia propõe uma concepção, muito mais parecida com o Código Civil brasileiro, que separa a responsabilidade para quem de fato foi o causador do dano, isto é, procede há uma análise estrita da existência de uma imprudência do programador quanto à blindagem de dados – política de *compliance* – que, em que pese a má-fé de um terceiro, o dever seria dele em cumprir a política ou, ainda, se há uma falha nos mecanismos de limitação da inteligência, forma com que a responsabilidade é igualmente sua, vez que falhou com o dever de prevenção aos riscos.

Bem fora apontado retro que a geração de um código mal intencionado e que gera um dano é, em verdade, uma legítima operação a qual não se presume falha do desenvolvedor, sobretudo ante à vasta possibilidade de utilização do código gerado, urgindo então a aplicação da *strict liability* definida na União Europeia em conjunto com o ideal de extrapolação da culpa civil do programador, nos termos aqui apresentados, para afastar sua responsabilidade e, assim, atingir, de fato, quem agiu de maneira torpe e efetivou o dano.

### 3 Considerações finais

Partindo da distinção técnica entre IAs determinísticas e IAs probabilísticas (notadamente LLMs), ficou claro que a natureza técnica da tecnologia condiciona, de modo decisivo, a aferição do nexos causal, a possibilidade de identificação elemento volitivo ou da desídia atribuível ao fornecedor ou usuário envolvidos na cadeia e, por conseguinte, a atribuição do dever de indenizar.

---

profundo – foram utilizados. Essa “opacidade” do código (efeito da caixa obscura) significa que não é fácil explicar o porquê do comportamento singular da IA em determinadas situações e é ainda mais difícil descobrir se esse comportamento está interligado a algum “defeito” no código ou algum desvio no processo de desenvolvimento. (Nossa tradução livre)

As regras gerais de responsabilidade do Código Civil, bem como a prevista no Código de Defesa do Consumidor, oferecem instrumentos parciais e insuficientes para aplicação aos danos que envolvem a utilização de IAs Conexistas. Com isso, tem-se que a aplicação automática e indiscriminada da responsabilidade objetiva aos fornecedores de IA, sob o fundamento de risco inerente à atividade, apresentam limitações práticas e jurídicas: nem toda Inteligência Artificial implica em risco inerente e nem sempre o dano decorre de conduta imputável exclusivamente ao desenvolvedor.

A experiência europeia consistente na incorporação do conceito de *strict liability* oferece importantes reflexões, uma vez que atrai a necessidade de padrões técnicos reforçados de diligência no momento de desenvolvimento da IA, assim como, com a adoção do referido regime, incumbe ao fornecedor comprovar que foram incorporadas à IA mecanismos de prevenção e limitação que

Neste cenário, caso um usuário, de forma maliciosa, utilize de uma plataforma de IA de forma a acarretar algum dano, a responsabilização deve ser pautada, inicialmente, na aferição das políticas de controle e segurança incorporadas à plataforma pelo desenvolvedor. Caso os parâmetros adotados estejam condizentes com os padrões técnicos exigidos, resta afastada a culpa do fornecedor, de modo que eventual responsabilização deve ser direcionada exclusivamente ao usuário.

A modernização da responsabilidade civil, portanto, não se trata de eliminar a culpa subjetiva, mas de reconhecer suas limitações probatórias em face da imprevisibilidade algorítmica. Neste novo cenário, cabe a modulação da responsabilização por meio de critérios materiais e procedimentais que incentivem a adoção de melhores práticas técnicas ao desenvolvedor das plataformas de IA.

A regulamentação deve evitar soluções de presunção absoluta de culpa que transfeririam, de forma indevida, riscos sistêmicos para atores que cumprem padrões de compliance e diligência. De outro lado, deve criar instrumentos que desestimulem comportamentos negligentes e punam omissões relevantes na adoção de medidas de prevenção.

Tem-se, portanto, seja pelos regramentos atuais ou pela incorporação de uma lógica semelhante à *strict liability*, que no caso eventual dano decorrente do mau uso intencional praticado por usuário em plataforma de IA, deve ser afastada a responsabilidade do fornecedor que demonstrou ter adotado políticas de segurança e controle condizentes com os padrões técnicos exigidos.

## Referências

HATTENHAUER, Hans. **Conceptos fundamentales del derecho civil: Introducción Histórico-Dogmática**. trad. espanhola Gonzalo Hernández. Barcelona: Ariel, 1987. 220p.

RUSSELL, Stuart J.; NORVIG, Peter. **Artificial Intelligence: A Modern Approach**. 4. ed. Upper Saddle River: Prentice Hall, 2020.

SCHREIBER, Anderson. **Novos paradigmas da responsabilidade civil: Da erosão dos filtros da reparação à duração dos danos**. 6. ed. São Paulo: Atlas, 2015. 280p.

STRYKER, Cole. **What are large language models (LLMs)?**. IBM: Nova Iorque, 10 set. 2025. Disponível em: <https://www.ibm.com/think/topics/large-language-models>. Acesso em: 21 set. 2025.

TEPEDINO, Gustavo; SILVA, Rodrigo da Guia (Coord.). **O Direito Civil na era da Inteligência Artificial**. São Paulo: Thomson Reuters Brasil/Revista dos Tribunais, 2020.

VAINZOF, Rony; GUTIERREZ, Andriei Guerrero (coord.). **Inteligência artificial: sociedade, economia e Estado**. São Paulo: Thomson Reuters Brasil, 2021.

WENDERHOST, Christiane. **Strict Liability for AI and other Emerging Technologies**. De Gruyter Brill: Berlim/Boston, 4 dez. 2020. Disponível em: <https://www.degruyterbrill.com/document/doi/10.1515/jetl-2020-0140/html>. Acesso em: 17 set. 2025.