IX ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS V

VIVIANNE RIGOLDI

JÉSSICA FACHIN

ROSANE TERESINHA PORTO

Copyright © 2026 Conselho Nacional de Pesquisa e Pós-Graduação em Direito

Todos os direitos reservados e protegidos. Nenhuma parte destes anais poderá ser reproduzida ou transmitida sejam quais forem os meios empregados sem prévia autorização dos editores.

Diretoria – CONPEDI
Presidente - Profa. Dra. Samyra Haydêe Dal Farra Naspolini - FMU – São Paulo
Diretor Executivo - Prof. Dr. Orides Mezzaroba - UFSC – Santa Catarina
Vice-presidente Norte - Prof. Dr. Jean Carlos Dias - Cesupa – Pará
Vice-presidente Centro-Oeste - Prof. Dr. José Querino Tavares Neto - UFG – Goiás
Vice-presidente Sul - Prof. Dr. Leonel Severo Rocha - Unisinos – Rio Grande do Sul
Vice-presidente Sudeste - Profa. Dra. Rosângela Lunardelli Cavallazzi - UFRJ/PUCRio – Rio de Janeiro
Vice-presidente Nordeste - Prof. Dr. Raymundo Juliano Feitosa - UNICAP - Pernambuco

Representante Discente: Prof. Dr. Abner da Silva Jaques - UPM/UNIGRAN - Mato Grosso do Sul

Conselho Fiscal:
Prof. Dr. José Filomeno de Moraes Filho - UFMA - Maranhão
Prof. Dr. Caio Augusto Souza Lara - SKEMA/ESDHC/UFMG - Minas Gerais
Prof. Dr. Valter Moura do Carmo - UFERSA - Rio Grande do Norte
Prof. Dr. Fernando Passos – UNIARA - São Paulo
Prof. Dr. Edinilson Donisete Machado - UNIVEM/UENP - São Paulo
Secretarias
Relações Institucionais:
Prof. Dra. Claudia Maria Barbosa - PUCPR - Paraná
Prof. Dr. Heron José de Santana Gordilho - UFBA - Bahia
Profa. Dra. Daniela Marques de Moraes - UNB - Distrito Federal
Comunicação:
Prof. Dr. Robison Tramontina - UNOESC - Santa Catarina
Prof. Dr. Liton Lanes Pilau Sobrinho - UPF/Univali - Rio Grande do Sul
Prof. Dr. Lucas Gonçalves da Silva - UFS - Sergipe
Relações Internacionais para o Continente Americano:
Prof. Dr. Jerônimo Siqueira Tybusch - UFSM - Rio Grande do sul
Prof. Dr. Paulo Roberto Barbosa Ramos - UFMA - Maranhão
Prof. Dr. Felipe Chiarello de Souza Pinto - UPM – São Paulo
Relações Internacionais para os demais Continentes:
Profa. Dra. Gina Vidal Marcilio Pompeu - UNIFOR - Ceará
Profa. Dra. Sandra Regina Martini - UNIRITTER / UFRGS - Rio Grande do Sul
Profa. Dra. Maria Claudia da Silva Antunes de Souza - UNIVALI – Santa Catarina
Educação Jurídica
Profa. Dra. Viviane Coêlho de Séllos Knoerr - Unicuritiba - PR
Prof. Dr. Rubens Beçak - USP - SP
Profa. Dra. Livia Gaigher Bosio Campello – UFMS – MS
Eventos:
Prof. Dr. Yuri Nathan da Costa Lannes - FDF - São Paulo
Profa. Dra. Norma Sueli Padilha - UFSC - Santa Catarina
Prof. Dr. Juraci Mourão Lopes Filho - UNICHRISTUS - Ceará

Comissão Especial
Prof. Dr. João Marcelo de Lima Assafim - UFRJ - RJ
Profa. Dra. Maria Creusa De Araújo Borges - UFPB - PB
Prof. Dr. Antônio Carlos Diniz Murta - Fumec - MG
Prof. Dr. Rogério Borba - UNIFACVEST - SC

D598

Direito, governança e novas tecnologias V [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Vivianne Rigoldi; Jéssica Fachin; Rosane Teresinha Porto – Florianópolis: CONPEDI, 2026.

Inclui bibliografia
ISBN: 978-65-5274-589-7
Modo de acesso: www.conpedi.org.br em publicações
Tema: Constituição, Processo e Justiça Social: o papel da jurisdição constitucional na efetivação de direitos

2. Direito. 3. Governança e novas tecnologias. IX Encontro Virtual do CONPEDI (2: 2026: Florianópolis, Brasil).

CDU: 34



Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

IX ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS V

Apresentação

O Conselho Nacional de Pesquisa e Pós-graduação em Direito (CONPEDI), referência na difusão de pesquisas que abordam os novos fenômenos envolvendo o Direito, firma-se como espaço qualificado para apresentação de pesquisas produzidas na área das novas tecnologias em face do Direito.

O tema, recorrente nos artigos apresentados - o uso da inteligência artificial no âmbito jurídico, demonstra que a maior sociedade científica na área jurídica do Brasil se mantém atenta às inovações tecnológicas, ao avanço de diversas tecnologias, novas experiências no judiciário e nos escritórios de advocacia. Artigos, de alta relevância acadêmica e científica, destacam que o Direito não está imune a essas transformações e reiteram a necessidade de atenção aos desafios regulatórios do uso da inteligência artificial no mundo jurídico.

Diferentes pesquisas, apresentadas no Grupo de Trabalho 'Direito, Governança e Novas Tecnologias V', alertam para os efeitos deletérios da opacidade algorítmica,

referindo-se à falta de transparência sobre como sistemas de inteligência artificial e seus algoritmos produzem decisões, dentro e fora do judiciário. Nos textos, a governança

digital é debatida, com rigorosa visão científica, objetivando garantir o uso estratégico de tecnologias de informação e comunicação para gerir serviços, promover a segurança

de dados e integrar processos, de forma transparente, eficiente, com foco na participação ativa do cidadão na tomada de decisões.

algorítmico e tecnológico do sistema de justiça, englobando a investigação de cibercrimes, a digitalização de procedimentos policiais e judiciais, provas digitais e a

regulação de plataformas para combater conteúdos ilícitos.

Destarte, os artigos apresentados e os debates produzidos no Grupo de Trabalho ‘Direito, Governança e Novas Tecnologias V’ são essenciais para o

fortalecimento das diretrizes nacionais de regulação das novas tecnologias, pela formação de parâmetros normativos e procedimentais adequados à proteção dos

direitos humanos e fundamentais, à garantia da segurança da informação, à gestão de riscos e ao fortalecimento da transparência e do alinhamento legal no uso das novas

tecnologias no âmbito jurídico.

Por essas razões, as coordenadoras do GT convidam para a leitura do teor integral dos artigos, agradecendo a participação dos autores pesquisadores desta edição.

Vivianne Rigoldi/Jéssica Fachin/Rosane Porto

RESPONSABILIDADE CIVIL OBJETIVA PELO RISCO E OS TRÊS REGIMES DE BECKERS E TEUBNER: POSSIBILIDADES DE RECEPÇÃO NO ORDENAMENTO JURÍDICO BRASILEIRO

STRICT LIABILITY FOR RISK AND THE THREE LIABILITY REGIMES OF BECKERS AND TEUBNER: POSSIBILITIES OF RECEPTION IN THE BRAZILIAN LEGAL ORDER

Guilherme De Sousa Cadorim
Cildo Giolo Junior
José Sérgio Saraiva

Resumo

A sociedade contemporânea é marcada pela disseminação de sistemas de inteligência artificial autônoma que tomam decisões com consequências jurídicas relevantes, desafiando os pressupostos estruturais da responsabilidade civil. O modelo clássico de imputação, fundado na conduta humana voluntária, no nexo causal linear e na identificabilidade do agente, revela-se insuficiente diante da opacidade algorítmica, da fragmentação da agência e dos riscos sistêmicos produzidos por tais sistemas. A cláusula geral de responsabilidade objetiva pelo risco prevista no Art. 927, parágrafo único, do CC/02 representa o principal vetor normativo disponível no ordenamento brasileiro, mas não oferece critérios suficientes para distinguir os diferentes tipos de risco da inteligência artificial nem para identificar os sujeitos responsáveis em cada hipótese. Diante dessa lacuna, este artigo investiga, por meio do método dedutivo e de abordagem qualitativa, a seguinte pergunta de pesquisa: considerando a responsabilidade civil objetiva pelo risco como aplicável aos danos causados por sistemas de inteligência artificial, seria possível a recepção dos três regimes propostos por Beckers e Teubner no ordenamento jurídico brasileiro? A análise demonstra que tais regimes encontram graus distintos de receptividade no direito brasileiro: o primeiro operacionalizável desde já por interpretação da cláusula geral de risco; o segundo parcialmente receptível mediante desenvolvimento doutrinário e legislativo; e o terceiro compatível com a tradição nacional de fundos setoriais de socialização de risco. Conclui-se

conduct, linear causation, and agent identifiability, proves insufficient in the face of algorithmic opacity, fragmented agency, and systemic risks produced by such systems. The general clause of strict liability for risk set forth in Article 927, sole paragraph, of the Brazilian Civil Code of 2002 constitutes the main normative instrument available in the Brazilian legal order, yet does not offer sufficient criteria for distinguishing the different types of risk posed by artificial intelligence or for identifying liable parties in each scenario. Against this backdrop, this article investigates, through a deductive method and qualitative approach, the following research question: considering strict liability for risk as applicable to damages caused by artificial intelligence systems, would it be possible to receive the three liability regimes proposed by Beckers and Teubner into the Brazilian legal order? The analysis demonstrates that such regimes find varying degrees of receptivity in Brazilian law: the first is already operational through interpretation of the general risk clause; the second is partially receptible through doctrinal and legislative development; and the third is compatible with Brazil's established tradition of sectoral risk socialization funds. The article concludes that reception of the theory contributes to filling doctrinal gaps and to building a regulatory framework combining effective victim protection, legal certainty, and encouragement of technological development in Brazil.

Keywords/Palabras-claves/Mots-clés: Artificial intelligence, Strict civil liability, Systemic risks, Liability regimes, Beckers and teubner

1 INTRODUÇÃO

A sociedade contemporânea experimenta uma transformação sem precedentes na estrutura das relações sociais e econômicas, impulsionada pela disseminação de sistemas de inteligência artificial capazes de tomar decisões autônomas, formular recomendações e executar tarefas de forma independente, sem intervenção humana direta e identificável. Algoritmos de aprendizado de máquina atuam hoje em setores críticos (por exemplo, saúde, crédito, mobilidade, segurança pública e mercados financeiros), produzindo consequências jurídicas relevantes para indivíduos e coletividades.

Esse cenário desafia os fundamentos sobre os quais repousa a responsabilidade civil brasileira. O modelo clássico de imputação, estruturado sobre a identificação de uma conduta humana voluntária, de um nexo causal linear e de um dano atribuível a agente determinado, pressupõe uma racionalidade humana subjacente ao ato lesivo. Quando o dano decorre de decisão autônoma de um sistema algorítmico, cujo funcionamento interno é opaco até mesmo para seus criadores, os instrumentos tradicionais de imputação parecem perdem aderência à realidade dos fatos e se mostrarem insuficientes.

O ordenamento jurídico brasileiro dispõe, no Art. 927, parágrafo único, do Código Civil de 2002, de uma cláusula geral de responsabilidade objetiva aplicável às atividades consideradas de risco para os direitos de outrem. Essa abertura normativa representa o principal vetor para a imputação de danos causados por sistemas de inteligência artificial no ordenamento vigente, diante da ausência de um marco regulatório para a IA.

Nesse contexto, a teoria dos três regimes de responsabilidade civil para a inteligência artificial, desenvolvida por Anna Beckers e Gunther Teubner, sobretudo na obra "*Three Liability Regimes for Artificial Intelligence: Algorithmic Actants, Hybrids, Crowds*", apresenta-se como referencial analítico oportuno e de especial relevância. A partir da tipologia de comportamento das máquinas elaborada nos estudos de tecnologia da informação, preditos autores propõem três regimes distintos de imputação, correspondentes a três formas de risco sistêmico: o risco de autonomia, decorrente de decisões independentes de agentes algorítmicos; o risco de associação, emergente da cooperação inextrincável entre humanos e algoritmos; e o risco de interconectividade, gerado pela operação em rede de algoritmos sem interferência humana direta.

Diante desse quadro, este artigo formula a seguinte pergunta de pesquisa: considerando a responsabilidade civil objetiva pelo risco como aplicável aos danos causados por sistemas de

inteligência artificial, seria possível a recepção dos três regimes de responsabilidade propostos por Beckers e Teubner no ordenamento jurídico brasileiro?

O objetivo geral é investigar a viabilidade de recepção dos três regimes de Beckers e Teubner no direito brasileiro, tendo como eixo normativo a cláusula geral de responsabilidade objetiva contida na norma do Art. 927, parágrafo único, do Código Civil de 2002. Para tanto, os objetivos específicos são: (1) examinar os fundamentos e os limites da responsabilidade civil objetiva pelo risco no direito brasileiro; (2) identificar e caracterizar os três riscos sistêmicos da inteligência artificial (IA) segundo Beckers e Teubner; (3) analisar os três regimes de responsabilidade propostos pelos autores; e (4) verificar a compatibilidade e os limites de sua recepção no ordenamento nacional.

A pesquisa adota abordagem qualitativa e método dedutivo, partindo dos princípios gerais da teoria de Beckers e Teubner para verificar sua compatibilidade com o ordenamento jurídico brasileiro. A justificativa científica e social assenta-se na lacuna dogmática e doutrinária existente: a teoria de Beckers e Teubner, acerca de uma questão que não possui norma jurídica especifica para regulação, e que tem sido amplamente difundida no debate internacional sobre responsabilidade civil e inteligência artificial, não foi ainda objeto de análise sistemática pela doutrina civilista brasileira, lacuna que o presente artigo se propõe a contribuir para suprir.

O trabalho está organizado em quatro seções. Inicialmente, examina-se o modelo clássico de responsabilidade civil e seus limites diante da inteligência artificial. Na sequência, analisa-se a teoria dos três regimes de Beckers e Teubner, com ênfase na tipologia de riscos e nos regimes correspondentes. Após, investiga-se a compatibilidade da teoria com o ordenamento brasileiro, especialmente à luz do Art. 927, parágrafo único, do Código Civil. Por fim, discute-se e apresentam-se as conclusões acerca (im)possibilidade de sua recepção no ordenamento jurídico brasileiro.

2 A INSUFICIÊNCIA DO MODELO CLÁSSICO DE RESPONSABILIDADE CIVIL DIANTE DA INTELIGÊNCIA ARTIFICIAL

2.1 Os pressupostos estruturais da responsabilidade civil e a inteligência artificial

A responsabilidade civil brasileira, consolidada no Código Civil de 2002, estrutura-se sobre três pressupostos fundamentais: a conduta humana (comissiva ou omissiva, voluntária e

imputável ao agente), o dano (que pode ser material ou moral) e o nexo de causalidade entre tais elementos. No regime subjetivo previsto no Art. 186 do CC, acrescenta-se ainda a esta fatura o elemento da culpa (*lato sensu*). No regime objetivo, prescinde-se da demonstração de culpa, bastando a prova do dano e do nexo causal, desde que o agente desenvolva atividade que, por sua natureza, implique risco para os direitos de outrem, nos termos do que dispõe o Art. 927, parágrafo único, do CC:

> 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.

Como se pode imaginar *prima facie* esses pressupostos foram historicamente desenvolvidos tendo em mente a figura do agente humano como único centro de imputação. Sistemas de IA, não eram sequer concebidos naquele momento legiferante, mas, como realidade recentemente, tensionam radicalmente esses pressupostos.

Sobre a conduta enquanto elemento estruturante da responsabilidade civil, Sílvio de Salvo Venosa elenca que "*o ato voluntário é, portanto, o primeiro pressuposto da responsabilidade civil. Esse conceito prende-se ao de imputabilidade, porque a voluntariedade desaparece ou torna-se ineficaz quando o agente é juridicamente irresponsável"* (2017, p. 455). Trata-se de uma concepção que articula vontade e imputação em um mesmo plano normativo, afastando qualquer leitura mecanicista da conduta e reforçando a necessidade de que o agir seja compreendido como manifestação consciente e juridicamente atribuível.

Acerca dessa compreensão, Cavalieri Filho leciona que conduta é todo "*comportamento voluntário que se exterioriza através de uma ação ou omissão, produzindo consequências jurídicas. A ação ou omissão é o aspecto físico, objetivo, da conduta, sendo a vontade o seu aspecto psicológico, ou subjetivo*" (2014, p. 38). Predita definição evidencia a dupla dimensão da conduta, ao distinguir seu aspecto externo (ação ou omissão) de seu elemento interno (vontade), revelando que o direito não se limita a observar o comportamento em sua materialidade, mas o qualifica a partir de um juízo normativo.

Desta feita verifica-se que a primeira tensão no tocante à responsabilidade civil perante a IA abrolha já no elemento conduta: algoritmos de aprendizado de máquina não são dotados

de conduta propriamente dita, eles executam meramente instruções predefinidas, mas operam mediante processos de inferência cuja lógica interna é frequentemente incompreensível até mesmo para seus próprios desenvolvedores, fenômeno conhecido como o problema da opacidade ou da "caixa-preta" e que pode interferir na conexão de atribuição (Beckers; Teubner, 2021, p. 48). Não há, nesse caso, a manifestação de uma vontade humana diretamente ligada ao ato lesivo, mas este ainda assim se verifica.

A título exemplificativo, imagine um sistema doméstico inteligente de monitoramento de segurança e acesso (dispositivo AIoT), programado para reconhecer padrões de presença e autorizar ou restringir o acesso à residência com base em dados biométricos, geolocalização e hábitos dos moradores. Em razão de uma alteração nos parâmetros de aprendizado do algoritmo, ou ainda uma atualização remota defeituosa, o sistema passa a classificar erroneamente um dos próprios moradores como um agente externo sem autorização para ingresso na residência, bloqueando seu acesso durante a madrugada. Diante da impossibilidade de ingresso e da ausência de meios alternativos imediatos, o indivíduo permanece exposto a condições adversas, vindo a sofrer dano (extra) patrimonial.

Nesse cenário, o evento danoso não pode ser reconduzido à uma conduta humana individual específica, como requer a ordem de imputação clássica, pois decorre da interação entre múltiplos elementos: a modelagem algorítmica desenvolvida, as atualizações implementadas pelo fornecedor, a infraestrutura de dados que alimenta o sistema e o próprio uso cotidiano do dispositivo. Assim, a decisão de bloqueio, embora produza efeitos concretos no mundo físico, emerge de um processo técnico autônomo e opaco, cuja lógica interna não é diretamente acessível ao usuário e talvez atribuível ao desenvolvedor.

Diante desse quadro, evidencia-se que a dificuldade não reside apenas em identificar quem agiu, mas em reconhecer que, em muitos casos, não há propriamente uma conduta humana individual que possa ser diretamente correlacionada ao resultado lesivo nos termos da lei, o que fragiliza a própria estrutura tradicional da imputação de responsabilidade civil fundada no ideal de ação ou omissão voluntária.

Fica patente que a autonomia algorítmica rompe o vínculo clássico entre vontade e resultado, deslocando o centro da imputação para além da decisão humana direta. A imprevisibilidade deixa de ser enxergada como exceção e passa a constituir um elemento intrínseco ao funcionamento do sistema de IA que nossa sociedade colocou em funcionamento.

Mas as tensões não se limitam somente a este elemento estruturante. Elencada a problemática na conduta, torna-se necessária a analise em relação ao dano, que se apresenta como núcleo estruturante da responsabilidade civil e fundamento último do instituto.

Inexistindo dano, não há que se cogitar de responsabilização, pois o dever de indenizar pressupõe, necessariamente, a ocorrência de uma lesão juridicamente relevante

A fragmentação da agência e a autonomia decisória dos sistemas de IA deslocam o problema da responsabilidade para além do elemento conduta, exigindo que a análise avance para o próprio resultado produzido. É, portanto, no elemento do dano, em sua configuração, extensão e natureza, que se revelam com maior nitidez os efeitos jurídicos dessas dinâmicas tecnológicas, impondo a necessidade de examinar como o Direito qualifica e responde a lesões que emergem de processos sociotécnicos complexos e difusos.

Diante desta premissa, é interessante elencar que Kate Crawford observa que os sistemas de IA não são mecanismos neutros, mas "*estão incorporados em mundos sociais, políticos, culturais e econômicos, moldados por humanos, instituições e imperativos que determinam o que fazem e como o fazem*" (Crawford, 2021, p. 211, tradução livre), o que tem implicação direta para a responsabilidade civil: os danos que tais sistemas produzem não emergem de falhas técnicas isoladas, mas correspondem ao resultado de escolhas de design que refletem e reproduzem estruturas de poder.

Ocorre que nesta concepção os danos podem vir a assumir formas que os institutos tradicionais e ordenamentos jurídicos sequer concebiam anteriormente, seja quantitativamente, seja qualitativamente. A este respeito, Schreiber explicita que "*às figuras mais comuns de dano não-patrimonial (dano à integridade psicofísica, dano estético, dano à saúde etc) vêm se somando outras de surgimento mais recentes e de classificação ainda um tanto assistemática"* (2013, p. 89).

Dentro deste pensamento é que já tem havido menções aos denominados danos algorítmicos, que em determinadas situações, a vítima sequer sabe que sofreu. Para exemplificar: sistemas de IA que integram os ecossistemas IoT (os AIoT) operam de forma invisível para o destinatário da decisão, por exemplo quando (1) o veículo conectado que, a partir dos dados de telemetria transmitidos continuamente à montadora e às seguradoras, classifica o condutor em categorias de risco que determinam tanto o valor do seguro quanto a eventual recusa de cobertura e não comunica ao motorista os parâmetros segundo os quais seu comportamento de condução foi avaliado e classificado; (2) o sistema de automação residencial que, conectado a sensores ambientais e a plataformas de seguros, considerando o tanto de vezes que uma determinada porta ficou aberta, recalibra em tempo real o perfil de risco do morador e eleva silenciosamente o valor do prêmio contratado, também não informando ao segurado que foi o padrão de comportamento captado pelos dispositivos da casa que motivou o ajuste.

Em todos esses casos, o dano de fato já se consumou, na forma de um *decisum* desfavorável, seja majoração tarifária ou de exclusão de cobertura, antes que a vítima tenha tido qualquer condição de identificar a sua origem algorítmica, questionar os critérios utilizados ou sequer suspeitar que foi o processamento automatizado de seus próprios dados, capturados pelos dispositivos que integram o seu cotidiano, que determinou o resultado que a prejudicou.

Tanto é assim que Frank Pasquale, em *"The Black Box Society"* elenca que "*decisões que podem ser erradas, tendenciosas ou destrutivas não podem ser corrigidas quando estão ocultas"* (Pasquale, 2015, p. 18). Essa afirmação, formulada no plano político e ético, tem equivalente preciso no plano da responsabilidade civil: a lesão que não podendo ser identificada em sua origem algorítmica, igualmente não poderá ser reparada segundo os instrumentos tradicionais do instituto. Esta invisibilidade da lesão, longe de ser um acidente, é em muitos casos um produto deliberado da arquitetura e de opacidade que caracteriza os sistemas como mencionado por Kate Crawford.

O resultado dessa conjugação entre invisibilidade individual do dano, inacessibilidade da evidência estatística agregada e opacidade estrutural do processo decisório é, em última análise, a criação de um ambiente em que a lesão algorítmica se autoperpetua sem resistência jurídica efetiva. E mais, o ordenamento jurídico, ao exigir que a vítima individual demonstre individualmente o que só pode ser demonstrado coletivamente, converte a assimetria informacional em imunidade de fato.

Em relação ao nexo causal, tem-se que os danos produzidos por sistemas algorítmicos em ambientes de alta complexidade computacional, como o ocorrido no *Flash crash* de 2010, em que houve quebra trilionária nas bolsas do mercado financeiro americano em apenas 36 minutos (Corporate Finance Institute, 2019), podem emergir de interações entre múltiplos algoritmos em velocidade que torne absolutamente a impossível uma precisa identificação de um nexo linear entre um ato específico e o resultado danoso (Beckers; Teubner, 2021, p. 4-5).

A opacidade algorítmica passa a representar mais do que um desafio técnico, ela figura obstáculo jurídico estruturante, na medida em que impede a reconstrução inteligível do percurso decisório que produziu o dano. A exigência clássica de demonstração do nexo causal contrasta, assim, em uma barreira epistêmica que favorece os detentores da tecnologia e fragiliza a posição das vítimas.

Passando ao elemento da culpa, previsto na modalidade de responsabilidade subjetiva, quando cotejado com hipóteses de falhas por sistemas de IA, a forma como tensiona os elementos estruturantes adquire contornos ainda mais agudos. A doutrina de Gustavo Tepedino, Aline Terra e Gisela Guedes, ao descrever a culpa normativa, ensinam que ela "*se revela na*

ideia de desvio de conduta, e cuja apreciação desconsidera a análise do perfil subjetivo do agente que se pretende responsabilizar, mas leva em conta o comportamento exigível diante das especiais circunstâncias do caso concreto" (2021, p. 204). Dessa feita, para que se possa falar em desvio de conduta a implicar culpa, será necessário que exista um padrão de conduta identificável: um arquétipo comportamental que funcione como parâmetro de comparação com o comportamento concreto do agente.

Tal padrão, nos sistemas tradicionais, é construído a partir da experiência social consolidada, das normas técnicas da atividade, dos usos e costumes do setor e das expectativas legítimas dos destinatários da atividade. No entanto, em sede de sistemas de aprendizado de máquina, a construção de qualquer padrão de conduta esbarra em dificuldades que não são meramente probatórias, mas até mesmo conceituais.

Em que consiste o comportamento tecnicamente adequado de um algoritmo de recomendação? Qual é o padrão de conduta de um sistema de iluminação automatizado? Essas perguntas não têm respostas consensuais na literatura técnica, tampouco no ordenamento jurídico, o que torna a aferição da culpa normativa estruturalmente indeterminada nas hipóteses de sistemas de IA.

Lawrence Lessig, na sua obra seminal sobre a relação entre código e direito, intitulada "*The Law of the Horse: what cyberlaw might teach",* já havia advertido que a arquitetura dos sistemas digitais não seria neutra, que ela incorporar valores e distribui o poder de modos que poderiam escapar às categorias jurídicas tradicionais. Isto porque na concepção dele o código, assim compreendido também o Direito, seria formado por um conjunto de restrições de comportamentos, previsto por determinados sujeitos, que listariam os possíveis e os que, pela incorporação de determinados valores ao sistema, seriam impossíveis (1999, p. 509).

Transposta para o contexto dos sistemas de IA, essa advertência revela que os sistemas algorítmicos não apenas executam funções técnicas, mas incorporam escolhas valorativas de alguém sobre o que é relevante, aceitável normal (ou não); escolhas que definem o próprio constructo sobre o qual padrão de conduta deveria ser explanado.

Assim, a própria ideia de culpa normativa perde seu ponto de apoio tradicional, uma vez que o padrão de conduta prescinde de um dado externo e compartilhado, criado coletivamente, para tornar-se inerente à arquitetura do sistema e de quem detém poder sobre o código. Isto posto a avaliação do desvio já não se realizaria por referência a um comportamento socialmente estabilizado e cuja tônica é relativamente pacífica, mas diante de parâmetros opacos e contingentes definidos no próprio código.

Diante destas tensões todas, nota-se que a IA não apenas desafia pontualmente os pressupostos da responsabilidade civil, mas coloca em crise a própria racionalidade sobre a qual o instituto foi historicamente estruturado. A lógica de imputação fundada na linearidade causal, na identificabilidade do agente e na cognoscibilidade do processo decisório revela-se insuficiente para apreender fenômenos marcados por opacidade, autonomia e complexidade sistêmica. Assim, mais do que adaptar categorias existentes, impõe-se repensar os próprios critérios de imputação, sob pena de se admitir a consolidação de espaços de irresponsabilidade jurídica em um contexto em que os danos se tornam cada vez mais difusos, invisíveis e estruturalmente incorporados ao funcionamento das tecnologias que permeiam a vida contemporânea

Torna-se necessário investigar então em que medida os mecanismos de responsabilidade objetiva já previstos no ordenamento jurídico brasileiro podem oferecer respostas mais adequadas a esses novos riscos tecnológicos. Nesse sentido, ganha relevo a cláusula geral de risco prevista no Art. 927, parágrafo único, do CC, cuja estrutura aberta e vocação expansiva podem permitir ao intérprete enfrentar situações em que a imputação subjetiva se mostra inviável ou insuficiente.

2.2 A cláusula geral de risco do Art. 927, parágrafo único, do Código Civil

Diante das limitações do regime subjetivo de responsabilidade civil que se mostraram historicamente, consistente sobretudo nas hipóteses de *probatio diabólica* (que não se pretende aprofundar neste estudo), alinhado com o pensamento da doutrina mundial, o legislador brasileiro adotou, no Art. 927, parágrafo único, do Código Civil de 2002, uma cláusula geral de responsabilidade objetiva fundada no risco da atividade. Trata-se de norma de textura aberta, que confia ao intérprete a qualificação hermenêutica das atividades de risco aptas a desencadear a imputação objetiva.

Consoante defendido por nomes expressivos da doutrina no âmbito da responsabilidade civil, "*o reconhecimento da configuração de atividades de risco a partir do emprego generalizado de sistemas de inteligência artificial parece a solução adequada, em linha de princípio, para o equacionamento da questão atinente à individualização do critério de imputação do regime de responsabilidade"* (Tepedino; Silva, 2019, p. 84).

Assim sendo, à semelhança do que outrora se verificava com atividades fruto do desenvolvimento tecnológico, o desenvolvimento e a operação de sistemas de IA podem ser enquadrados como atividade de risco para fins do parágrafo único do Art. 927 do CC, ainda que se considere tais atividades lícitas e socialmente úteis.

Contudo, a aplicação da cláusula geral de risco à inteligência artificial esbarra em um problema estrutural: ela pressupõe que seja possível identificar o agente responsável, estabelecer o nexo causal entre sua atividade e o dano, e definir o regime de reparação aplicável. Quando o dano decorre de decisões emergentes de redes complexas de algoritmos interconectados, como por exemplo ocorrido no *Flash Crash,* sem que seja possível identificar qual nó da rede produziu o resultado lesivo, a cláusula geral de risco, interpretada nos moldes tradicionais, revela-se insuficiente.

Desta feita, seria necessário preencher, portanto, uma lacuna normativa que a cláusula geral de risco não supre integralmente: ela oferece uma abertura interpretativa valiosa, mas não fornece os critérios para distinguir os diferentes tipos de risco produzidos pela inteligência artificial, nem para identificar os sujeitos responsáveis em cada hipótese. É precisamente essa lacuna que a teoria de Beckers e Teubner se propõe a preencher.

3 A TEORIA DOS TRÊS REGIMES DE RESPONSABILIDADE PARA A INTELIGÊNCIA ARTIFICIAL: BECKERS E TEUBNER

3.1 A tipologia de comportamento das máquinas e as instituições sociodigitais

Anna Beckers, professora de Direito Privado e Metodologia Jurídica da Universidade de Maastricht, e Gunther Teubner, professor emérito de Direito Privado e Sociologia Jurídica da Universidade Goethe de Frankfurt, publicaram em 2021, pela editora Hart Publishing, a obra "*Three Liability Regimes for Artificial Intelligence: Algorithmic Actants, Hybrids, Crowds*". O livro propõe uma abordagem interdisciplinar inédita para o problema da responsabilidade civil por danos causados por sistemas de inteligência artificial, combinando estudos de tecnologia da informação, teoria sociológica e análise comparada do direito civil em sistemas de *common law* e *civil law*.

A obra parte do diagnóstico de que os ordenamentos jurídicos contemporâneos enfrentam lacunas crescentes de responsabilidade diante da autonomia algorítmica; lacunas estas que nem mesmo a responsabilidade subjetiva, nem a responsabilidade objetiva clássica,

nem a responsabilidade pelo produto seriam capazes de suprir integralmente. De modo que propõe, em resposta, três regimes distintos de imputação calibrados às diferentes formas de risco que a inteligência artificial produz em contextos sociais específicos (Beckers; Teubner, 2021, p. v-vi).

A teoria de Beckers e Teubner parte, portanto, de uma premissa epistemológica fundamental: os riscos produzidos por sistemas de inteligência artificial não derivam simplesmente das propriedades técnicas dos algoritmos, mas emergem da integração desses algoritmos em diferentes contextos sociais (Beckers; Teubner, 2025, p. 310). Essa perspectiva evita o que os autores denominam de "*curto-circuito tecnodeterminista*", isto é, a falácia de inferir normas jurídicas diretamente de propriedades técnicas dos sistemas computacionais (2021, p. 14).

O ponto de partida é uma tipologia desenvolvida nos estudos de tecnologia da informação que distingue três tipos de comportamento das máquinas: o comportamento individual de máquina, o comportamento coletivo de máquina e o comportamento híbrido humano-máquina (Beckers; Teubner, 2021, p. 17-18).

Para que essa tipologia possa orientar o Direito, contudo, é necessário introduzir as "*instituições sociodigitais*" (socio-digital institutions) como variáveis intermediárias entre tecnologia e direito. Segundo explicam os autores, constituem instituições sociodigitais todos aqueles "(...)*complexos estabilizados de expectativas sociais que, no nosso caso, são expectativas em relação ao comportamento de algoritmos em contextos sociais. Tais instituições não são idênticas aos sistemas sociais nem às organizações formais ou relações sociais*." (Beckers, Teubner, 2025, p. 310, tradução livre)[1].

Esta noção de instituições sociodigitais permite deslocar o eixo analítico da tecnologia em si para o plano das estruturas sociais que estabilizam expectativas acerca do comportamento algorítmico, o que representa uma inflexão teórica relevante para o problema da responsabilidade civil. Em outras palavras: não se trata de conceber a IA como um mero artefato técnico inserido em relações jurídicas pré-existentes, mas de reconhecer que sua integração nos contextos sociais produz formas institucionalizadas de interação que reorganizam os próprios pressupostos da imputação.

Deste modo, tais instituições configuram-se como complexos normativamente estruturados de expectativas sociais acerca da atuação de algoritmos em contextos específicos,

[1] No original: "*Socio-digital institutions mean stabilized complexes of social expectations, which, in our case, are expectations regarding the behaviour of algorithms in social contexts. Such institutions are neither identical with social systems nor with formal organizations, or social relations."*

não se confundindo nem com sistemas sociais amplos, nem com organizações formais, nem com relações interpessoais isoladas, mas operando como formas intermediárias de acoplamento estrutural entre sistemas técnicos e sociais (Beckers; Teubner, 2025, p. 310).

Essa formulação possui implicações diretas para o Direito, pois evidencia que a responsabilidade civil não pode mais ser pensada exclusivamente a partir de sujeitos individuais e condutas isoladas, mas deve ser reconstruída à luz dos contextos institucionais nos quais os algoritmos são empregados.

Neste particular, elencam os autores que cada tipo de comportamento algorítmico corresponde à uma instituição sociodigital específica, que engendra um tipo particular de risco e demanda um regime de responsabilidade próprio: (1) o comportamento individual de máquina realiza-se na instituição da assistência digital, gerando o risco de autonomia; (2) o comportamento híbrido produz a instituição da associação humano-máquina, gerando o risco de associação; e (3) o comportamento coletivo de máquina opera na instituição da exposição à interconectividade, gerando o risco de interconectividade (Beckers; Teubner, 2023, p. 86-90). Essa estrutura tripartite constitui o núcleo da teoria e será examinada nas subseções seguintes de forma fracionada.

3.2 O risco de autonomia e a responsabilidade vicária: assistência digital

O primeiro tipo de risco, denominado pelos autores de risco de autonomia, emerge do comportamento individual das máquinas no contexto da instituição sociodigital de assistência digital (*digital assistance)*. Nessa configuração, um algoritmo atua como agente autônomo (actante) em nome de um agente principal humano, tomando decisões independentes que vinculam ou afetam juridicamente esse principal e terceiros (Beckers; Teubner, 2025, p. 311).

A introdução do conceito de actante revela-se relevante por romper com a concepção instrumental clássica que reduz a tecnologia a um meio neutro de execução da vontade humana. O actante algorítmico não apenas executa comandos, mas opera com graus de autonomia que lhe permitem produzir decisões não antecipadas por seus criadores ou usuários. Embora essa autonomia não elimine o nexo causal, ela fragiliza o vínculo tradicional de imputação, na medida em que o comportamento do sistema já não pode ser diretamente reconduzido à vontade de um agente humano identificável (Beckers; Teubner, 2025, p. 315).

A instituição sociodigital subjacente é a da representação, transplantada do domínio humano para o domínio digital: o algoritmo age “como se” fosse o principal, mas com graus de liberdade que tornam suas decisões imprevisíveis (Beckers; Teubner, 2021, p. 87-88).

É nesse contexto que a teoria da responsabilidade vicária assume centralidade analítica na obra dos autores. Beckers e Teubner sustentam que a relação entre usuário e algoritmo pode ser compreendida a partir da lógica agente principal-actante, na qual o sistema atua como se fosse o próprio titular da decisão, embora verdadeiramente não seja.

A figura da *potestas vicaria* revela, nesse sentido, que a atuação do actante, seja ele humano ou algorítmico, não apenas substitui, mas constitui juridicamente a vontade do agente principal, produzindo efeitos que lhe são imputáveis (Beckers; Teubner, 2025, p. 314).

Essa reconstrução teórica é particularmente sofisticada porque evita duas soluções simplistas que frequentemente aparecem no debate contemporâneo: de um lado, a equiparação plena dos algoritmos a sujeitos jurídicos, com atribuição de personalidade, mas sem dotação e patrimônio; de outro, sua redução a meros instrumentos, incapazes de gerar imputação própria.

Entre esses extremos, a proposta dos autores consiste em reconhecer uma forma limitada de agência algorítmica, suficiente para justificar a aplicação de regimes de responsabilidade vicária, mas não a ponto de romper completamente com a centralidade da imputação humana. A consequência dessa construção é a redefinição do sujeito responsável.

Assim, por exemplo, o usuário que habilita, em seu assistente virtual (como a *Alexa*), a funcionalidade de compras por voz, inclusive a partir de sugestões automatizadas do próprio sistema, estará a assumir o risco decorrente dessa delegação ampliada de capacidade decisória. Ao permitir que o sistema não apenas execute comandos, mas também proponha e concretize aquisições de assinaturas, músicas e/ou audiolivros e livros, com base em padrões inferidos de consumo, o usuário passa a integrar uma instituição sociodigital em que o algoritmo atua como actante na formação da decisão dele (agente principal). Não lhe seria dado, posteriormente, pretender afastar integralmente os efeitos dessas operações sob o argumento de ausência de manifestação direta de vontade, pois foi sua própria configuração inicial que instituiu o regime de atuação autônoma e, com isso, internalizou o risco correspondente.

Os autores destacam que esse regime não responsabiliza uma multiplicidade de atores envolvidos (desenvolvedores, programadores, fabricantes, comerciantes etc), mas tão somente o usuário que delega uma tarefa à IA e assim assume o risco de decisão autônoma desta, sendo o único responsável pelas falhas daí advindas (Beckers; Teubner, 2023, p. 90-91).

As condições para sua aplicação são: (a) que haja delegação de tarefa por agente principal humano a um actante algoritmo; (b) exigência de que a delegação requeira decisões autônomas; (c) ação ilícita do actante sem que fosse previsível ou explicável pelo desenvolvedor; (d) ação do agente principal constitutiva de violação de dever de cuidado; e (e) causalidade entre ação e dano (Beckers; Teubner, 2023, p. 94).

3.3 O risco de associação e a responsabilidade empresarial em rede: hibridismo digital

O segundo tipo de risco, intitulado de risco de associação, advém do comportamento híbrido, no qual humanos e algoritmos interagem de forma tão inextrincável que não é sequer dado distinguir contribuições individuais de cada um destes na produção do resultado danoso. A instituição sociodigital correspondente é a "*associação humano-máquina*": um coletivo emergente, dotado de propriedades que não se reduzem à soma das contribuições individuais de seus membros humanos e algorítmicos.

Como os autores explicam, no contexto dos híbridos a decisão não pode ser atribuída exclusivamente ao usuário nem ao algoritmo, pois decorre de um processo conjunto em que *inputs* humanos e *outputs* algorítmicos se entrelaçaram de forma indissociável. Trata-se de uma agência compartilhada, na qual a distinção clássica entre sujeito e instrumento deixa de ser possível de analisar, exigindo a reconstrução da imputação a partir da interdependência das contribuições envolvidas (Beckers; Teubner, 2025, p. 317-318).

Trata-se, nessa modalidade, de risco de associação, que surge quando atividades humanas e algorítmicas se entrelaçam de forma indissociável, impedindo a atribuição de responsabilidade individual, pois o dano decorre de propriedades emergentes do coletivo (Beckers; Teubner, 2025, p. 311).

Nessas hipóteses, a responsabilidade vicária, fundada na lógica principal-agente, mostra-se insuficiente, já que pressupõe um centro unitário de vontade, o que não se verifica nos arranjos híbridos. Em seu lugar, observa-se uma unidade operativa composta, na qual humano e algoritmo participam conjuntamente do resultado, sem hierarquia clara.

Nesse contexto, a imputação deve ser reconstruída sob uma lógica de corresponsabilidade funcional, em que a atribuição do dano decorre da participação integrada na atividade de risco, e não da identificação de um autor principal (Beckers; Teubner, 2025, p. 318). Os exemplos mobilizados pelos autores são particularmente elucidativos:

> Panama Papers: O jornalismo investigativo frequentemente faz uso de algoritmos. Em uma investigação complexa, um consórcio internacional de jornalistas tem trabalhado de forma colaborativa com ajuda tecnológica para identificar práticas fiscais ilegais de empresas e indivíduos. A dificuldade do trabalho investigativo era o vasto número de documentos que precisavam ser analisados. Os algoritmos realizaram o trabalho de etiquetar, categorizar e selecionar os textos relevantes. Os humanos então revisaram o trabalho deles. Além disso, a posterior publicação do trabalho nas notícias e sua distribuição como notícia também se torna influenciada pelos algoritmos na priorização e nas decisões de filtragem. Os Panama Papers demonstram como algoritmos e jornalistas podem trabalhar bem juntos para revelar um escândalo que, de

> outra forma, nunca teria se tornado público. No entanto, tal prática tem um vasto potencial de danos. E se tal investigação estivesse culpando e envergonhando uma pessoa ou uma empresa que não estivesse envolvida? Se um erro algorítmico tivesse ocorrido, a assistência digital se aplica. No entanto, e se um erro algorítmico não for claramente delineável, mas a cooperação entre investigação humana e cálculo algorítmico levou à acusação equivocada? Para complicar ainda mais, dado os algoritmos envolvidos na distribuição de notícias, tais acusações falsas poderiam facilmente se espalhar e se tornar um grande tema de notícia. (Beckers, Teubern, 2021, p. 160, tradução livre)

Outro exemplo ainda é o da governança corporativa digitalizada, em que algoritmos integram conselhos de administração e tomam decisões em conjunto com diretores humanos, como o caso da Crescera Capital (Braun, 2026), a responsabilidade pelo ato coletivo não pode ser individualmente imputada

Para esse risco, os autores propõem o regime de responsabilidade empresarial em rede (*enterprise liability/network liability*), inspirado na *enterprise liability* americana e na *Gesamthandshaftung* alemã. O regime funciona em dois passos: primeiro, o ato ilícito é atribuído ao híbrido como ator coletivo; segundo,a responsabilidade pelo ato coletivo é canalizada aos membros da rede, com base em sua participação econômica e no controle exercido sobre o híbrido. A responsabilidade proporcional dos nós da rede é determinada segundo a "*network-share liability"*, isto é, uma responsabilidade de participação na rede, analogamente à *market-share liability* (Beckers; Teubner, 2021, p. 131-132).

3.4 O risco de interconectividade e o fundo coletivo: comportamento coletivo das máquinas

O terceiro e mais desafiador dos riscos, denominado de risco de interconectividade, emerge do comportamento coletivo de máquinas e sistemas de IA, quando algoritmos operam de forma interconectada, sem qualquer interferência humana direta, produzindo dados e danos sistêmicos que nenhum ator individual pode prever, controlar ou vincular a um nexo causal determinado. Entrementes: a ação deixa de ser híbrida para assumir caráter propriamente sistêmico, marcado pela interação descentralizada entre múltiplos agentes humanos e não humanos, cujas dinâmicas escapam à reconstrução analítica linear.

Nessas hipóteses, o dano já não decorre de uma decisão singular ou de uma relação bilateral específica, mas emerge de uma rede de interações distribuídas, frequentemente intermediadas por sistemas distintos que operam em múltiplos níveis e segundo finalidades diversas (Beckers; Teubner, 2025, p. 319-320).

Esse risco de interconectividade se manifesta quando algoritmos passam a atuar em verdadeiros "enxames operacionais" (*swarm*), sem intervenção humana identificável, produzindo comportamentos coletivos cujos efeitos lesivos não podem ser reconduzidos, de forma precisa, a qualquer componente individual do sistema (Beckers; Teubner, 2024, p. 312).

Tal tipologia ganha relevo especial quando cotejada com a sociedade de risco descrita por Ulrich Beck, na qual os riscos deixam de se apresentar como eventos isolados para assumir a condição de efeitos estruturais do próprio modelo de desenvolvimento, ocultos sob uma indiscernibilidade que dificulta sua percepção direta pelas vítimas e pela sociedade (Beck, 2011, p. 32).

Os autores exemplificam essa hipótese a partir de mercados automatizados e sistemas financeiros algorítmicos, nos quais múltiplos algoritmos realizam operações de compra e venda em velocidades elevadíssimas, produzindo efeitos que escapam à capacidade de previsão e controle de qualquer agente individual. O comportamento emergente dessas redes não pode ser fragmentado em contribuições causais individualizadas, o que reforça a insuficiência das categorias clássicas de imputação assentadas na causalidade linear (Beckers; Teubner, 2025, p. 320).

O caso paradigmático, consoante mencionado, foi o *Flash Crash,* nos EUA, em 2010, quando o Departamento de Justiça atribuiu a um único *trader*, Navinder Sarao, a responsabilidade pela quebra do mercado já que o algoritmo deste inseria ordens falsas para induzir outros sistemas automatizados a seguir determinada tendência de negociação, permitindo posterior lucro com a reversão estratégica. Embora as investigações tenham identificado a prática de *spoofing* como fator indireto do colapso, não foi possível precisar em que ponto a conduta ilícita se materializou dentro da cadeia algorítmica automatizada (Beckers; Teubner, 2021, p. 162).

Para enfrentar essa realidade, Beckers e Teubner propõem uma reconfiguração mais profunda da responsabilidade civil, orientada pela noção de imputação sistêmica. Em vez de concentrar esforços na identificação de um responsável individual, a imputação passaria a considerar a inserção dos agentes em estruturas institucionais produtoras e distribuidoras de risco. O foco desloca-se, portanto, da conduta isolada para a participação em sistemas de risco, permitindo reconectar o dano às esferas de controle e benefício mesmo quando a cadeia causal não puder ser reconstruída de forma linear (Beckers; Teubner, 2025, p. 320-321).

Para esse risco, os autores propõem um regime de fundo coletivo (*fund liability*), financiado pelo setor industrial envolvido, calculado com base na participação de mercado e na capacidade de resolução de problemas de cada ator. O modelo inspirador é o Superfund

ambiental americano, o 42 US Code § 9601ff (United States of America, 1980), que distribui custos de remediação a toda uma indústria com base no benefício econômico extraído de atividade geradora de riscos coletivos. A lógica subjacente é a de que, quando a atribuição de ação, causalidade e responsabilidade é impossível, a solução não pode ser ignorar os danos, mas socializar os riscos de forma proporcional aos benefícios auferidos (Beckers; Teubner, 2023, p. 92-93).

Expostos os regimes delineados pelos autores, impõe-se na sequência verificar em que medida essas construções teóricas podem ser recepcionadas pelo ordenamento jurídico brasileiro, especialmente diante da estrutura dogmática da responsabilidade civil prevista no Código Civil de 2002.

4 COMPATIBILIDADE E LIMITES DA RECEPÇÃO DA TEORIA DE BECKERS & TEUBNER NO ORDENAMENTO JURÍDICO BRASILEIRO

4.1 O primeiro regime: responsabilidade vicária e o Art. 927, parágrafo único, do CC

O regime da responsabilidade vicária do usuário/operador pelo risco de autonomia apresenta a expressiva compatibilidade com o direito civil brasileiro vigente. A cláusula geral de risco do Art. 927, parágrafo único, do CC Civil, aplicada ao desenvolvedor ou operador de um sistema de IA que delega decisões autônomas a algoritmos, pode ser interpretada de modo a abranger exatamente a hipótese que Beckers e Teubner identificam como a mais comum de dano por inteligência artificial: a delegação de tarefas a agentes autônomos que produzem resultados lesivos imprevisíveis.

A analogia com a responsabilidade do empregador pelos atos do empregado, prevista no Art. 932, III, do Código Civil, reforça essa possibilidade. Quem se beneficia economicamente da delegação de decisões a sistemas algorítmicos e assume o risco inerente a essa delegação deve responder objetivamente pelos danos produzidos, independentemente de culpa. Também há que se lembrar da máxima *ubi emolumentum, ibi onus* (onde está o proveito, aí deve estar o encargo), o que é plenamente aplicável à exploração de atividades baseadas em inteligência artificial.

A recepção desse regime enfrenta, contudo, um desafio técnico relevante: a necessidade de se identificar o "usuário/operador" responsável em situações nas quais a cadeia de atores envolvidos na implantação de um sistema de IA seja extensa e fragmentada. A teoria de Beckers e Teubner, como exposto, para aumento de sua contribuição já oferece critério de que a responsabilidade recairia exclusivamente sobre aquele que delegou a tarefa à IA e assumiu

o risco de sua autonomia decisória, não sobre toda a cadeia produtiva, que permanece sujeita às regras da responsabilidade pelo produto.

4.2 O segundo regime: responsabilidade em rede e o direito brasileiro

O regime de risco de associação, por sua vez, representa o ponto de maior inovação da teoria dos autores em relação ao direito civil brasileiro vigente. Isso porque o ordenamento nacional não conta com um regime geral de responsabilidade coletiva por redes de atores que, individualmente, não praticaram ato ilícito, mas cujas contribuições conjuntamente produziram o dano.

Não obstante, elementos do direito positivo brasileiro ofereçam pontos de apoio para a construção desse regime, como a teoria da solidariedade passiva (CC, arts. 264 e seguintes) e a responsabilidade solidária dos fornecedores na cadeia de consumo (CDC, Art. 7º, parágrafo único), as quais demonstram que o ordenamento nacional já reconhece formas de responsabilidade coletiva em contextos de ação conjunta, inexiste um mecanismo de atribuição como seria proposto pelos autores.

O desafio principal estaria, portanto, na inexistência de mecanismo formal de atribuição de ação a um coletivo híbrido humano-algorítmico e de subsequente canalização proporcional da responsabilidade aos membros da rede. A recepção plena desse regime exigiria uma intervenção legislativa, mas sua aplicação parcial, especialmente no que diz respeito à responsabilidade solidária dos integrantes de uma rede de atores beneficiários de um sistema de IA híbrido, já pode ser construída hermeneuticamente a partir das normas vigentes.

4.3 O terceiro regime: o fundo coletivo e a tradição brasileira de socialização de riscos

O regime de risco de interconectividade pode encontrar no direito brasileiro tradição normativa consolidada na técnica legislativa dos fundos setoriais de socialização de risco, facilitando a sua implementação. Vale destacar a existência diversos exemplos de fundos de socialização de riscos nacionais: DPVAT, FGTS, FGC e os fundos garantidores do sistema financeiro habitacional.

Isto somente evidencia que o ordenamento nacional já domina, de certa maneira, os elementos estruturais que Beckers e Teubner propõem para um fundo de IA: isto é custeio proporcional por setor econômico; administração por autoridade regulatória; acesso das vítimas mediante critérios predefinidos, e; distribuição coletiva de riscos cuja imputação individual seria impossível ou antieconômica. O que falta, portanto, não é o modelo, mas sua transposição para a realidade específica de domínio da inteligência artificial.

A criação de um fundo setorial de responsabilidade por danos de IA, com custeio calculado com base na participação de mercado e na capacidade de resolução de problemas de cada ator, conforme proposto por Beckers e Teubner (2023, p. 92), não constituiria assim uma inovação estrutural para o direito pátrio propriamente dita, mas aplicação de uma lógica normativa já sedimentada a um novo domínio tecnológico. Nesse cenário, o PL 2.338/2023, ainda em tramitação na Câmara dos Deputados, destinado a ser o marco regulatório da IA, representa uma oportunidade normativa relevante. Embora, em sua redação, não preveja mecanismos de fundo coletivo para hipóteses de interconectividade sistêmica, a inclusão dessas disposições seria tecnicamente viável e doutrinalmente fundamentada.

Há ainda um argumento de política legislativa que merece a devida abordagem: a existência de regras claras sobre a distribuição de riscos sistêmicos da IA reduz a incerteza regulatória e, sob a perspectiva da análise econômica do direito, pode funcionar como fator de atração de investimentos no setor. Desenvolvedores e operadores de sistemas de inteligência artificial em larga escala necessitam de previsibilidade sobre o custo das externalidades sistêmicas de sua atividade. A existência de fundo com critérios transparentes de custeio e acesso é, sob esse ângulo, mais favorável ao ambiente de negócios e ao desenvolvimento tecnológico nacional do que um vácuo normativo que mantém o risco sistêmico inteiramente indefinido.

A recepção do terceiro regime, longe de onerar o desenvolvimento da IA no Brasil, poderia vir a constituir um dos pilares de um marco regulatório que combine proteção efetiva das vítimas de riscos sistêmicos com a previsibilidade necessária para consolidar o ecossistema brasileiro de inovação em IA.

5 CONCLUSÕES

O presente artigo investigou a viabilidade de recepção dos três regimes de responsabilidade para a inteligência artificial propostos por Beckers e Teubner no ordenamento jurídico brasileiro, tendo como eixo normativo a responsabilidade civil objetiva pelo risco prevista no Art. 927, parágrafo único, do CCódigo Civil de 2002.

A análise desenvolvida ao longo deste artigo permitiu confirmar a hipótese central da pesquisa: os pressupostos clássicos da responsabilidade civil mostram-se estruturalmente insuficientes para responder às formas de dano produzidas por sistemas de inteligência artificial autônoma. A lógica tradicional de imputação, fundada na identificabilidade de uma conduta humana, na linearidade causal e na cognoscibilidade do processo decisório, perde capacidade explicativa diante de fenômenos marcados por opacidade algorítmica, fragmentação da agência

e emergência de riscos sistêmicos. Embora a cláusula geral de risco prevista no Art. 927, parágrafo único, do Código Civil represente importante abertura normativa, sua estrutura aberta não oferece, por si só, critérios suficientes para distinguir os diferentes tipos de risco produzidos pela inteligência artificial nem para definir os sujeitos responsáveis em contextos de alta complexidade tecnológica.

Nesse cenário, a teoria de Beckers e Teubner revelou-se particularmente relevante ao propor uma reconstrução funcional da responsabilidade civil a partir da morfologia específica dos riscos algorítmicos. A tipologia tripartite formulada pelos autores (risco de autonomia, risco de associação e risco de interconectividade) evita tanto a insuficiência de modelos uniformes quanto a fragmentação excessiva de soluções casuísticas, ao estabelecer regimes de imputação calibrados às instituições sociodigitais em que os algoritmos operam. A contribuição central da teoria consiste precisamente em deslocar o foco da análise da tecnologia em abstrato para os contextos institucionais de integração dos sistemas algorítmicos, permitindo compreender que os danos produzidos pela IA não decorrem apenas de propriedades técnicas dos algoritmos, mas das formas sociais de sua utilização e inserção operacional.

A investigação demonstrou, ademais, que os três regimes propostos pelos autores encontram diferentes graus de receptividade no ordenamento jurídico brasileiro. O regime de responsabilidade vicária pelo risco de autonomia pode ser operacionalizado desde logo mediante hermenêutica da cláusula geral de risco do Código Civil, especialmente quando o usuário/ delegar decisões autônomas a sistemas algorítmicos. O regime de responsabilidade em rede pelo risco de associação, embora não encontre disciplina expressa, dialoga com institutos já conhecidos do direito brasileiro, como a solidariedade passiva e determinadas formas de responsabilidade coletiva, ainda que demande desenvolvimento legislativo e doutrinário para plena operacionalização. Já o regime de fundos coletivo para o risco de interconectividade figura compatível com tradição normativa nacional de socialização setorial de riscos, evidenciada em mecanismos como o DPVAT, FGTS, FGC, o que demonstra que a lógica proposta por Beckers e Teubner não representa ruptura absoluta com a experiência jurídica brasileira.

Por fim, a pesquisa permitiu concluir que a recepção desses regimes transcende uma discussão estritamente dogmática acerca da responsabilidade civil, reconfigurando-a: a construção de critérios normativos claros para distribuição dos riscos produzidos pela IA constitui também elemento relevante de política regulatória e desenvolvimento tecnológico. A ausência de parâmetros definidos de imputação não favorece a inovação, mas perpetua insegurança jurídica tanto para vítimas quanto para agentes econômicos envolvidos no

desenvolvimento de sistemas algorítmicos. A definição de regimes proporcionais aos diferentes riscos da IA, ao contrário, tende a produzir ambiente regulatório mais previsível, apto a conciliar proteção efetiva de direitos fundamentais, segurança jurídica e estímulo ao desenvolvimento sustentável da IA no Brasil.

REFERÊNCIAS

BECKERS, Anna; TEUBNER, Gunther. **Three Liability Regimes for Artificial Intelligence: Algorithmic Actants, Hybrids, Crowds**. Oxford: Hart Publishing, 2021.

BECKERS, Anna; TEUBNER, Gunther. **Responsibility for Algorithmic Misconduct: Unity or Fragmentation of Liability Regimes?** Yale Journal of Law and Technology, New Haven, v. 25, p. 76-100, 2023.

BECKERS, Anna; TEUBNER, Gunther. **The Risk-based Responsibility for Algorithmic Failures.** In: CREMONA, Marise (ed.). New Technologies and EU Law. Oxford: Oxford University Press, 2025. p. 307-327.

BRASIL. Lei n. 10.406, de 10 de janeiro de 2002. **Código Civil.** Diário Oficial da União, Brasília, DF, 11 jan. 2002.

BRASIL. Lei n. 8.078, de 11 de setembro de 1990. **Código de Defesa do Consumidor.** Diário Oficial da União, Brasília, DF, 12 set. 1990.

BRAUN, Daniela. **Agente de IA chega às reuniões do conselho de administração**. Valor Investe, São Paulo, 7 abr. 2026. Disponível em: Valor Investe. Acesso em: 16 maio 2026.

CAVALIERI FILHO, Sergio. **Programa de Responsabilidade Civil**. 11. ed. São Paulo: Atlas, 2014.

CORPORATE FINANCE INSTITUTE. **2010 flash crash**. [S. l.]: CFI Education Inc., 2019. Disponível em: <https://corporatefinanceinstitute.com/resources/equities/2010-flash-crash/>. Acesso em: 15 mai 2026

CRAWFORD, Kate. **Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence**. New Haven: Yale University Press, 2021.

SCHREIBER, Anderson. **Novos Paradigmas da Responsabilidade Civil: da erosão dos filtros da reparação à diluição dos danos**. 5. ed. São Paulo: Atlas, 2013.

TEPEDINO, Gustavo; SILVA, Rodrigo da Guia. Desafios da inteligência artificial em matéria de responsabilidade civil. **Revista Brasileira de Direito Civil**, *[S. l.]*, v. 21, n. 03, p. 61, 2019. Disponível em: https://rbdcivil.ibdcivil.org.br/rbdc/article/view/465. Acesso em: 15 mai. 2026.

VENOSA, Sílvio de Salvo. **Direito civil: obrigações e responsabilidade civil.** 17. ed. São Paulo: Atlas, 2017.