

IX ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS I

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 - UFRSA - Rio Grande do Norte

Prof. Dr. Fernando Passos - UNIARA - São Paulo

Prof. Dr. Ednilson 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

D597

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

Coordenadores: Rubens Beçak; Aires Jose Rover; Ana Elisa Silva Fernandes Vieira – Florianópolis: CONPEDI, 2026.

Inclui bibliografia

ISBN: 978-65-5274-592-7

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



IX ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS I

Apresentação

Os encontros nacionais do Conselho Nacional de Pesquisa e Pós-graduação em Direito (CONPEDI) têm se consolidado como referência na disseminação de pesquisas que abordam os novos fenômenos envolvendo o direito, e o Grupo de Trabalho "Direito, Governança e Novas Tecnologias" é um exemplo vivo desse compromisso. Nesta edição, o evento destacou-se não apenas pela qualidade dos trabalhos apresentados, mas pela presença de renomados professores pesquisadores em instigante debate com seus alunos de pós-graduação.

Como de praxe, houve uma diversidade muito grande de temas e abordagens. Numa tentativa de dar unidade temática e facilitar a compreensão dessa complexa teia de inovações, os coordenadores organizaram os artigos desta publicação em três grandes grupos de reflexão.

O primeiro bloco abordou o tema da "Inteligência Artificial, Viés Algorítmico e Responsabilidade Tecnológica". As reflexões apresentadas neste eixo evidenciam a tensão constante entre a rápida expansão da inteligência artificial - que transforma desde o papel da advocacia e o uso de "smart contracts" até a governança das plataformas digitais - e os profundos riscos sociais intrínsecos a essas tecnologias. Os debates trouxeram à tona denúncias contundentes sobre o racismo estrutural e algorítmico, demonstrando como projetos de cidades inteligentes e ferramentas de reconhecimento facial podem operar sob uma lógica de necropolítica se não houver um olhar crítico. Consequentemente, os pesquisadores debruçaram-se sobre a urgência de estabelecer novos marcos de regulação, modelos de responsabilidade civil e robustos mecanismos de "compliance" e segurança da informação para frear a discriminação e garantir proteção contratual.

destaque para a urgência de uma identidade digital segura e a afirmação de um Estatuto da Criança e do Adolescente (ECA) no ambiente virtual.

Por fim, o terceiro bloco englobou "Direitos Humanos, Processo Judicial, Economia Digital e Governança Institucional". Este eixo refletiu de forma abrangente as complexas interseções entre a Revolução 4.0 e a proteção da dignidade humana. Foram problematizados fenômenos contemporâneos alarmantes, como a precarização das relações na "gig economy", o abandono parental no ambiente virtual e a violação do direito ao esquecimento infantil decorrente do "oversharenting". Em paralelo a essas vulnerabilidades, os estudos investigaram a modernização das estruturas institucionais e econômicas. Discutiu-se desde a responsabilidade civil frente à tokenização e financeirização de terras no agronegócio, até o esforço contínuo para democratizar o sistema de justiça. Para isso, foram apresentadas análises valiosas sobre a implantação municipal do processo eletrônico, a aplicação do "design thinking" no direito e o aprimoramento da transparência e da participação democrática sob a ótica do direito comparado.

Os artigos que ora são apresentados ao público têm a finalidade de fomentar a pesquisa e fortalecer o diálogo interdisciplinar em torno das respostas que o Direito precisa dar a uma realidade em constante e veloz transformação.

Enfim, os coordenadores do GT convidam os leitores para desfrutarem do teor integral dos artigos, expressando imensa gratidão pela participação dos autores pesquisadores desta edição.

Os Coordenadores

Prof. Dr. Aires José Rover, Universidade Federal de Santa Catarina

Prof. Dr. .Rubens Beçak, Universidade de São Paulo - USP

SMART CONTRACTS COMO NOVA TECNOLOGIA: RESPONSABILIDADE CIVIL NAS PLATAFORMAS DIGITAIS E O TRIPÉ DE COMPLIANCE, AUDITORIA E SEGURANÇA DA INFORMAÇÃO

SMART CONTRACTS AS A NEW TECHNOLOGY: CIVIL LIABILITY IN DIGITAL PLATFORMS AND THE TRIPOD OF COMPLIANCE, AUDITING AND INFORMATION SECURITY

Amanda Ribeiro Soares ¹
Flavia Suzy Dias Holderegger ²
Sergio Iglesias Nunes de Souza ³

Resumo

Este artigo analisa se o ordenamento jurídico brasileiro é apto a fundamentar a imputação de responsabilidade civil por danos decorrentes de smart contracts, considerando a lacuna normativa existente e a complexidade técnica do nexo causal sob assimetria informacional. Adotou-se método dedutivo e direito comparado, em especial o AI Act europeu e o PL brasileiro nº 2.338/2023. Demonstra-se que a responsabilidade objetiva (art. 927, parágrafo único, do CC) é dogmaticamente operativa, desde que articulada à governança tecnológica. A investigação revela que o entrave principal não é a ausência normativa, mas a opacidade técnica que dificulta a prova judicial. Assim, os Programas de Compliance, Auditoria e Segurança da Informação tornam-se essenciais para constituir suporte probatório à apreciação judicial. Conclui-se que, embora o Projeto de Lei nº 2.338/2023 avance ao prever a inversão do ônus da prova, permanece omissivo quanto às especificidades dos smart contracts, lacuna que demanda enfrentamento doutrinário sistemático. A principal contribuição científica reside em demonstrar, mediante encadeamento dedutivo articulado, que o Direito Civil brasileiro dispõe de mecanismos normativos suficientemente flexíveis para enfrentar os riscos jurídicos associados aos smart contracts, desde que interpretados de forma sistemática e acompanhados de estruturas eficazes de governança tecnológica.

Palavras-chave: Smart contracts, Responsabilidade civil objetiva, Direitos da personalidade, Programas de conformidade, Plataformas digitais

Abstract/Resumen/Résumé

This article examines whether the Brazilian legal system is capable of grounding the attribution of civil liability for damages arising from smart contracts, considering the existing regulatory gap and the technical complexity of establishing causation under informational asymmetry. A deductive method and comparative law were adopted, with particular attention to the European AI Act and Brazilian Bill No. 2,338/2023. It is demonstrated that strict liability (Article 927, sole paragraph, of the Civil Code) is dogmatically operative, provided it is articulated with technological governance. The investigation reveals that the main obstacle is not the absence of regulation, but rather technical opacity, which hinders judicial proof. Accordingly, Compliance, Audit, and Information Security Programs become essential to provide evidentiary support for judicial assessment. It is concluded that although Bill No. 2,338/2023 represents progress by providing the reversal of the burden of proof, it remains silent regarding the specificities of smart contracts; a gap that calls for systematic doctrinal engagement. The main scientific contribution lies in demonstrating, through an articulated deductive reasoning, that Brazilian Civil Law provides sufficiently flexible normative mechanisms to address the legal risks associated with smart contracts, provided they are interpreted systematically and supported by effective technological governance structures.

Keywords/Palabras-claves/Mots-clés: Smart contracts, Strict liability, Personality rights, Conformity programs, Digital platforms

1 INTRODUÇÃO

A popularização dos *smart contracts* em plataformas digitais e da sua natureza autoexecutável fomentou o debate sobre a responsabilidade civil decorrente de danos patrimoniais e violações aos direitos da personalidade, tornando-se imperativo avaliar os mecanismos de reparação existentes e se as legislações que respaldam os direitos dos usuários afetados e as estruturas corporativas voltadas à prevenção de riscos são suficientes para resguardar direitos.

A cibercultura, longe de representar uma era futura, constitui a forma sociocultural vigente, fruto da simbiose entre a cultura contemporânea e as tecnologias digitais, e impõe ao direito a tarefa de readequar seus instrumentos tradicionais de imputação e tutela (LEMOS, 2023). Essa readequação não pressupõe a superação dos institutos clássicos, mas a investigação de sua capacidade de responder, com suficiência normativa, aos fenômenos tecnológicos emergentes.

Os *smart contracts*, em sua estrutura típica, não se confundem com sistemas de inteligência artificial. Eles operam, em regra, de forma determinística, a partir de comandos condicionais previamente definidos (*if/then*), sem aprendizado autônomo ou comportamento adaptativo. A opacidade algorítmica, frequentemente mencionada nos debates contemporâneos, não é inerente a todos os *smart contracts*, mas tende a se intensificar em contextos nos quais tais instrumentos se encontram integrados a sistemas de inteligência artificial, especialmente aqueles baseados em *machine learning* ou *deep learning* (KORKMAZ, 2024). Essa diferenciação é metodologicamente relevante, pois a investigação aqui empreendida tem como objeto contratos autoexecutáveis em sentido estrito, ainda que se reconheça a possibilidade de hibridização tecnológica em arquiteturas mais sofisticadas.

A consolidação das relações jurídicas no meio digital impõe a releitura dos instrumentos clássicos do Direito Civil, tendo em vista que a disciplina ordinária da responsabilidade civil oferece fundamentos normativos relevantes para o equacionamento dos danos causados por sistemas autônomos, em uma postura que repele soluções automáticas e privilegia a elasticidade interpretativa (TEPEDINO; SILVA, 2020). Trata-se de investigar em que medida as categorias do Direito Civil ainda respondem, com adequação funcional, aos fenômenos tecnológicos contemporâneos, dentre os quais os *smart contracts*.

Sob essa ótica, o problema de pesquisa pode ser assim formulado: ‘em que medida o ordenamento jurídico brasileiro oferece instrumentos adequados para a imputação de responsabilidade civil pelos danos resultantes da execução autônoma de *smart contracts*, tendo

em vista a ausência de regulação específica e a complexidade técnica envolvida na demonstração do nexo causal?’

A relevância do questionamento intensifica-se quando se observa que o Projeto de Lei nº 2.338/2023 (BRASIL, 2023), embora estabeleça a Avaliação de Impacto Algorítmico, a análise dos impactos de sistemas de Inteligência Artificial sobre direitos fundamentais, com previsão de medidas preventivas, mitigadoras e potencializadoras, nada dispõe sobre os *smart contracts*. Tal omissão transfere aos operadores do direito o ônus de integrar a lacuna a partir dos institutos civis vigentes, o que justifica a centralidade conferida à referida proposição legislativa neste estudo.

A partir desse recorte, o trabalho estrutura-se em torno dos seguintes objetivos específicos: (i) examinar a função preventiva dos Departamentos de Conformidade (*Compliance*), Auditoria e Segurança da Informação na governança dos riscos associados aos *smart contracts*, de modo a identificar mecanismos privados de mitigação capazes de complementar a tutela jurídica; (ii) enfrentar o desafio probatório inerente à demonstração do nexo causal, cuja complexidade técnica frequentemente exige perícias especializadas, sob pena de inviabilizar a efetiva tutela dos direitos das vítimas; e (iii) evidenciar a defasagem do processo legislativo brasileiro em relação à velocidade das transformações tecnológicas, recorrendo, subsidiariamente, ao direito comparado, em especial ao Regulamento (UE) 2024/1689 (*AI Act*) (UNIÃO EUROPEIA, 2024), como parâmetro normativo apto a inspirar soluções compatíveis com a realidade nacional.

A pesquisa parte da hipótese de que, embora inexista regulação específica dos *smart contracts* no ordenamento jurídico brasileiro, o arcabouço normativo vigente, especialmente a cláusula geral de responsabilidade objetiva prevista no art. 927, parágrafo único, do Código Civil (BRASIL, 2002) em diálogo sistemático com o Código de Defesa do Consumidor (BRASIL, 1990) e com a Lei Geral de Proteção de Dados (BRASIL, 2018), pode revelar-se dogmaticamente idôneo para fundamentar a imputação de responsabilidade civil por danos decorrentes da execução automatizada desses contratos. Referida idoneidade não é afirmada de forma irrestrita: condiciona-se à presença de mecanismos técnicos e organizacionais aptos a mitigar assimetrias informacionais, assegurar transparência e viabilizar a adequada produção probatória.

Quanto à justificativa, parte-se do papel do Estado diante das inovações tecnológicas contemporâneas, quando o Estado opta pela inação, dificilmente se pode falar em neutralidade normativa, uma vez que o silêncio regulatório tende a produzir impactos mais gravosos sobre posições jurídicas estruturalmente mais vulneráveis (CASTELLS, 2005). No campo

tecnológico, a ausência de regras não atinge todos de modo homogêneo, mas penaliza, em regra, os elos mais vulneráveis da cadeia. Werthein (WERTHEIN, 2000) adverte que o determinismo e o evolucionismo tecnológicos distorcem a análise do complexo processo de mudança social alimentando atitudes contemplativas diante de transformações que reclamam resposta ativa do direito. É justamente nessa direção, voltada à construção de uma resposta jurídica ativa às transformações digitais, que o presente trabalho situa sua contribuição.

No que diz respeito aos *smart contracts*, esse desequilíbrio tende a se intensificar, sobretudo quando tais instrumentos se encontram integrados a sistemas algorítmicos mais complexos, utilizados para tomada de decisões automatizadas em plataformas digitais. Estudos sobre opacidade algorítmica e dificuldade de explicabilidade de sistemas computacionais complexos, como os desenvolvidos por Korkmaz (KORKMAZ, 2024, p. 117-119), embora situados originalmente no campo da ciência da computação, contribuem para evidenciar os limites práticos de compreensão e auditabilidade desses sistemas por usuários externos. Essa limitação técnica, quando transposta ao plano jurídico, pode agravar as dificuldades enfrentadas pelas vítimas na reconstrução fática do dano e na demonstração do nexo causal, especialmente em ambientes fortemente automatizados.

Este artigo utiliza o método proposto por Feferbaum e Queiroz (FEFERBAUM; QUEIROZ, 2019, p. 43-44), autores que sistematizam técnicas e abordagens para a elaboração de trabalhos científicos na seara jurídica. A partir dos parâmetros ali delineados, orienta-se a investigação pelo emprego articulado da legislação, doutrina nacional e estrangeira e direito comparado, em pesquisa bibliográfica e documental, pautada por análise informada, fundamentada, ponderada e desinteressada.

A hipótese é examinada ao longo do trabalho mediante raciocínio dedutivo explícito, que parte das premissas normativas gerais do sistema de responsabilidade civil para avaliar sua incidência concreta sobre o uso de *smart contracts* em plataformas digitais de trabalho. Assume centralidade, nesse percurso, a cláusula geral do referido diploma civil (BRASIL, 2002), segundo a qual aquele que exerce atividade que implique risco para os direitos de outrem responde pelos danos causados independentemente de culpa.

Com base nessa premissa, analisa-se em que medida a automação contratual, marcada pela rigidez técnica e pela assimetria técnica, pode atrair a responsabilidade civil objetiva (BRASIL, 2002). Sustenta-se que, diante da dificuldade de correções *ex post* e da escala dos danos potenciais, é possível aplicar o regime jurídico vigente mediante adaptações interpretativas, desde que a análise seja reforçada por mecanismos de prevenção, como programas de *Compliance*, auditorias técnicas e políticas de segurança da informação.

Delineados o problema, a hipótese, os objetivos, a justificativa e os contornos metodológicos, percorre-se, a partir deste ponto, o itinerário argumentativo que conduz à resposta do questionamento central proposto.

2 *SMART CONTRACTS* – CONCEITO E APLICABILIDADE COMO NOVA TECNOLOGIA

2.1 Conceito e funcionamento: da criptografia ao protocolo autoexecutável

As tecnologias disruptivas têm pressionado o direito contratual a repensar suas bases, sobretudo diante da automação crescente de obrigações jurídicas. Nesse panorama, os *smart contracts* passam a ocupar lugar relevante na reconfiguração das relações negociais contemporâneas, não apenas sob o prisma da eficiência econômica, mas também em razão dos desafios jurídicos que suscitam, em especial no tocante à imputação de responsabilidade por danos decorrentes de sua execução automatizada.

Conforme a definição proposta por (SZABO, 1994), esses instrumentos consistem em protocolos informatizados destinados à execução automatizada dos termos contratuais, concebidos para realizar condições previamente estipuladas, reduzir exceções e diminuir a dependência de intermediários de confiança. Essa formulação inicial foi posteriormente aprofundada pelo autor, que passou a descrevê-los como contratos digitais capazes de formalizar relações jurídicas por meio do uso combinado de algoritmos e técnicas criptográficas, incorporáveis tanto em *hardware* quanto em *software*, com o propósito de tornar o inadimplemento economicamente desvantajoso para o devedor (SZABO, 1996).

A compreensão desse fenômeno exige situá-lo no contexto da sociedade da informação, cujo paradigma técnico-econômico tem como fator-chave não mais os insumos de energia, mas os insumos baratos de informação, com alta penetrabilidade em todas as atividades humanas, individuais e coletivas (WERTHEIN, 2000). A técnica deixa de ser um pano de fundo estável para se tornar uma cena de constante metamorfose, reconfigurando as bases do funcionamento social e das atividades cognitivas (LÉVY, 1993).

A disseminação da tecnologia *blockchain* como infraestrutura subjacente aos *smart contracts* consolidou esse paradigma. De Filippi; Wright (DE FILIPPI; WRIGHT, 2018) descrevem esses contratos como código autoexecutável embarcado em redes *blockchain*, capaz de fazer cumprir acordos automaticamente quando condições predefinidas são satisfeitas, inaugurando o que os autores denominam regra do código, expressão utilizada para designar

formas de regulação técnica que passam a coexistir e interagir com os mecanismos jurídicos tradicionais, sem necessariamente substituí-los.

No plano operacional, os *smart contracts* estruturam-se a partir da conjugação de elementos técnicos que lhes conferem viabilidade e segurança. Destaca-se inicialmente a criptografia assimétrica, baseada no uso de chaves públicas e privadas, cuja função é assegurar tanto a autenticidade das partes envolvidas quanto a integridade das informações objeto da transação (NAKAMOTO, 2008).

Essa infraestrutura técnica, embora responsável por elevados níveis de segurança e imutabilidade, implica significativo grau de complexidade, sobretudo para usuários não especializados, limitação que tende a se intensificar quando os *smart contracts* se encontram integrados a sistemas algorítmicos mais complexos, hipótese em que emergem desafios adicionais de explicabilidade e produção probatória, examinados a seguir.

2.2 Opacidade algorítmica e riscos jurídicos dos *smart contracts*

O mesmo atributo que torna os *smart contracts* eficientes, a sua capacidade de se executar sem intervenção humana, é também a origem dos seus riscos jurídicos mais relevantes. Os *smart contracts*, em sua configuração típica, não constituem sistemas de inteligência artificial, na medida em que operam, geralmente, a partir de lógica condicional determinística previamente programada. O uso de técnicas como *machine learning*, *deep learning* e redes neurais capazes de produzir decisões automatizadas de difícil explicação inclusive para seus próprios desenvolvedores não é inerente aos *smart contracts*, mas pode ocorrer em contextos nos quais estes se encontrem integrados a sistemas algorítmicos mais sofisticados (KORKMAZ, 2024). É justamente nesses ambientes híbridos que os riscos tendem a se intensificar.

Nesses contextos, ganha relevo o fenômeno da chamada opacidade algorítmica, que segundo Burrell (*apud* KORKMAZ, 2024), apresenta três dimensões distintas e que agravam estruturalmente as assimetrias informacionais entre quem desenvolve a tecnologia e quem é por ela afetado: a intencional (proteção corporativa por ocultação); a técnica (escrever e ler código são habilidades restritas a especialistas); e a matemática (descompasso entre a otimização em alta dimensão do aprendizado de máquina e as demandas da racionalidade humana).

Diante disso, a transparência não pode ser concebida como um fim em si mesma, mas como condição instrumental e pressuposto para os mecanismos de responsabilização e para os arranjos preventivos a serem examinados adiante (KORKMAZ, 2024). Como adverte Rodotà (*apud* KORKMAZ, 2024), o cidadão nasce não mais livre, mas perfilado, prisioneiro de

mecanismos que não conhece ou não pode controlar o que configura desapropriação tecnológica de prerrogativas humanas, potencializada por desnível de poder não solucionável exclusivamente pela atribuição ao interessado do dever de se atentar a esses processos.

No plano da governança tecnológica, Pinheiro (PINHEIRO, 2024) propõe o modelo “4R” receita, risco, responsabilidade e regulamentação, partindo da premissa de que para toda receita há risco e responsabilidade correspondentes. Para a autora, é fundamental investir em campanhas educativas para o usuário final e em equipes preparadas para delimitar os limites da responsabilidade de cada parte. Inovação e responsabilidade são, sob essa perspectiva, faces da mesma moeda: se uma ferramenta tecnológica tem o poder de afetar inúmeras pessoas, quem a produz não pode se eximir da correspondente responsabilização.

Sob ângulo estrutural, o denominado formalismo algorítmico entendido como adesão a regras e formas prescritas que, embora úteis para abstrair e definir processos analíticos, tendem a ignorar a complexidade social do mundo real revela que o código de um *smart contract* opera, em regra, com base em lógica condicional rígida e de difícil reversão (KORKMAZ, 2024). Em regra, satisfeitas as condições previamente programadas, a execução ocorre de forma automática, independentemente de circunstâncias que, no direito contratual clássico, poderiam autorizar a revisão ou a resolução do negócio jurídico, como vício de consentimento ou desequilíbrio superveniente.

Convém observar, no entanto, que, embora o registro do código em *blockchain* imponha elevado grau de rigidez e resistência à modificação, não se pode afirmar a absoluta impossibilidade de intervenção.

Embora existam soluções técnicas que admitem graus limitados de controle *ex post* tais como contratos atualizáveis (*upgradeable contracts*), mecanismos de governança *on-chain*, oráculos e funções de interrupção previamente programadas (*circuit breakers*), tais mecanismos dependem de escolhas técnicas *ex ante* e não afastam os riscos de execução automática de difícil reversão. Em regra, portanto, há significativa limitação à intervenção, sobretudo em arquiteturas estritamente imutáveis, sem que se trate, contudo, de impossibilidade absoluta.

É precisamente diante dessas limitações que a responsabilidade civil assume papel central como instrumento de tutela. Tepedino; Silva (TEPEDINO; SILVA, 2020) defendem que o regime ordinário da responsabilidade civil fornece fundamentos normativos relevantes para a imputação de danos causados por sistemas tecnológicos automatizados, desde que interpretado de modo funcional e sistemático. Não se sustenta a suficiência automática do regime vigente, mas reconhece-se sua aptidão dogmática para adaptação aos riscos da automação contratual, mesmo sem regulação específica.

Como conclusão parcial desta seção, atendendo ao objetivo (i) e (ii) na medida em que mapeia os riscos juridicamente relevantes, sustenta-se que os *smart contracts*, embora distintos dos sistemas de inteligência artificial, ostentam características técnicas (rigidez, automatismo, opacidade contextual) que os aproximam, em determinados arranjos, do conceito normativo de atividade de risco, abrindo caminho à análise dogmática desenvolvida na seção seguinte.

2.3 *Smart contracts* nas plataformas digitais e a lacuna normativa brasileira

Nas plataformas digitais de trabalho, o problema é concreto: pagamentos variáveis, bonificações e metas são calculados e executados automaticamente por algoritmos, sem que o trabalhador compreenda como a decisão foi tomada e sem condições reais de contestá-la, já que isso exigiria acesso ao código-fonte e conhecimento técnico que a parte mais vulnerável da relação, em regra, não detém.

O ordenamento brasileiro já havia dado sinais de que essa proteção é necessária. Como observa Korkmaz (KORKMAZ, 2024), as decisões automatizadas foram endereçadas no Brasil, inicialmente, por intermédio de regulação setorial a Lei do Cadastro Positivo (Lei nº 12.414/2011) é exemplo disso, ao prever o direito à revisão de decisões exclusivamente automatizadas, demonstrando que a ausência de regulação específica sobre *smart contracts* não é lacuna por descuido, mas omissão que cabe aos operadores do direito suprir mediante os princípios gerais. Nessa direção, a Estratégia Brasileira de Inteligência Artificial reconheceu expressamente que sistemas de inteligência artificial devem ser centrados no ser humano e que a intervenção humana pode ser importante fator de mitigação do risco em decisões automatizadas de alto risco para os titulares (KORKMAZ, 2024).

O Projeto de Lei nº 2.338/2023, aprovado pelo Senado Federal em dezembro de 2024 e atualmente em tramitação na Câmara dos Deputados, embora contemple a Avaliação de Impacto Algorítmico para sistemas classificados como de alto risco, não disciplina de modo específico os *smart contracts*, o que reafirma a necessidade de recorrer aos instrumentos clássicos do Direito Civil. Nesse contexto, os arts. 113, 421 e 422 do Código Civil que consagram, respectivamente, a interpretação conforme a boa-fé, a função social do contrato e a boa-fé objetiva assumem função central como parâmetros jurídicos aptos a conter excessos do automatismo contratual, sem inviabilizar a inovação tecnológica.

3 RESPONSABILIDADE CIVIL E DIREITOS DA PERSONALIDADE NAS PLATAFORMAS DIGITAIS

3.1 Premissas normativas: art. 927, parágrafo único, do Código Civil

A responsabilidade civil, nesse contexto, exerce função subsidiária, pois seu viés compensatório individual nem sempre se mostra adequado a riscos coletivos, como os associados à inteligência artificial em larga escala, o que reforça a centralidade de arranjos preventivos (KORKMAZ, 2024), especialmente Programas de Conformidade e de gestão de riscos com supervisão humana. A automação contratual por *smart contracts* pode afetar direitos da personalidade protegidos pelos arts. 1º, III, e 5º, X, da CF/1988 e pelos arts. 11 a 21 do Código Civil, cuja violação pode gerar dever de reparação nos termos dos arts. 186 e 927, parágrafo único.

À luz dessas considerações, verifica-se que a automação contratual desafia os modelos tradicionais de imputação jurídica, exigindo uma leitura sistemática da responsabilidade civil que reconheça tanto seus limites estruturais quanto sua função de tutela dos direitos fundamentais. A combinação entre risco tecnológico, decisões automatizadas e assimetria informacional demanda a articulação de mecanismos preventivos e reparatórios, a fim de proteger a pessoa afetada sem comprometer de forma desproporcional a funcionalidade econômica dos *smart contracts*. Esse equilíbrio é central para a compreensão dogmática do tema e fundamenta a análise dos regimes jurídicos concorrentes examinados a seguir.

3.2 Regimes concorrentes de responsabilidade: Código Civil, Código de Defesa do Consumidor e Lei Geral de Proteção de Dados

Antes de avançar para a análise dogmática da hipótese de incidência da responsabilidade objetiva, mostra-se conveniente delimitar, de forma sistematizada, os três principais regimes normativos concorrentes que podem incidir sobre os danos decorrentes da execução automatizada de *smart contracts* em plataformas digitais. A sobreposição entre esses regimes não é incomum, mas exige operação interpretativa cuidadosa para evitar antinomias e garantir a tutela mais efetiva dos direitos atingidos.

O critério orientador da incidência tende a observar a seguinte lógica: havendo relação de consumo, aplicam-se preferencialmente as regras do CDC, sem prejuízo da incidência subsidiária do Código Civil; havendo tratamento de dados pessoais, incidem as regras da LGPD em caráter complementar; e, na ausência de relação de consumo e fora do âmbito da proteção de dados, opera o regime geral do Código Civil. Em todas as hipóteses, é possível diálogo das fontes, tendo em vista a unidade material do sistema de responsabilidade civil.

Quanto à inversão do ônus da prova, sua incidência depende, em regra, da verificação de dois critérios fundamentais: a hipossuficiência (técnica, informacional ou econômica) da parte autora e a verossimilhança das alegações. Esses parâmetros, já sedimentados na

jurisprudência consumerista, encontram terreno particularmente fértil nos litígios envolvendo *smart contracts*, em que a complexidade técnica e a opacidade contextual do código tendem a impossibilitar, em muitos casos, a produção de prova técnica pela parte hipossuficiente. O Projeto de Lei nº 2.338/2023, ao prever explicitamente a inversão do ônus da prova em seus arts. 35 a 37, reforça tendência já consolidada no ordenamento, sem inaugurar inovação absoluta.

3.3 *Smart contracts* e atividade de risco: análise dogmática

A potencial violação de direitos decorrente da automação contratual encontra ilustração analógica no caso analisado pelo Tribunal Superior do Trabalho no Informativo nº 291/2024, em que o bloqueio algorítmico do CPF de um trabalhador foi reconhecido como dano moral *in re ipsa* (BRASIL, 2024). Cumpre advertir, contudo, que o referido caso não envolve diretamente *smart contracts*, mas decisões automatizadas em contexto distinto, motivo pelo qual sua invocação se dá a título analógico, e não como precedente especificamente aplicável ao objeto deste estudo. A analogia, todavia, mostra-se relevante: tanto no caso analisado pelo TST quanto nos litígios envolvendo *smart contracts*, o que está em causa é o impacto de decisões automatizadas e/ou opacas sobre a autodeterminação do indivíduo.

Em um outro paralelo, cabe observar que a Lei Geral de Proteção de Dados Brasileira reforça essa proteção ao consagrar a autodeterminação informativa como fundamento do tratamento de dados (art. 2º, II) e ao exigir que as decisões automatizadas respeitem os princípios da não discriminação e da qualidade dos dados (art. 6º, IV). No âmbito regulatório comparado, o Regulamento UE 2024/1689 (*AI Act*) constitui hoje o mais amplo marco normativo sobre inteligência artificial em vigor, adotando lógica baseada em risco e classificando como de risco elevado os sistemas voltados à gestão e avaliação de trabalhadores. Embora não trate especificamente de *smart contracts*, o regulamento impõe obrigações de transparência, auditabilidade e registro que, por analogia, podem alcançar contratos inteligentes utilizados para automatizar métricas de desempenho, pagamentos variáveis e bonificações em plataformas digitais de trabalho.

O *AI Act* vai além da mera regulamentação técnica, ao oferecer parâmetros graduados que levam em conta a natureza e a complexidade de cada sistema, influenciando também a imputação de responsabilidade civil (NETA; NUNES, 2024). A quem for afetado por decisão de sistema classificado como de alto risco assegura-se o direito de obter explicações adequadas sobre seus fundamentos, especialmente quando houver impacto relevante sobre direitos fundamentais prerrogativa que encontra respaldo no art. 20 da Lei Geral de Proteção de Dados.

No plano nacional, o Projeto de Lei nº 2.338/2023 prevê a Avaliação de Impacto Algorítmico para sistemas de alto risco, em aproximação com a estrutura do modelo europeu. Em análise comparativa entre o *AI Act* da União Europeia e o Projeto de Lei brasileiro, Barbosa (BARBOSA, 2024) observa que ambos os diplomas estruturam-se a partir de níveis de risco, mas se afastam em um ponto central: enquanto o modelo europeu optou predominantemente pela responsabilidade subjetiva, o projeto brasileiro avança ao prever, em seu art. 27, hipótese de responsabilidade objetiva para sistemas de alto risco, opção que a autora reputa meritória, embora critique a limitação da responsabilização à participação no dano, por considerá-la presa a uma lógica causalista cuja superação dogmática se impõe.

Todavia, assim como o *AI Act*, o projeto não disciplina de forma específica as peculiaridades dos *smart contracts*, o que impede sua aplicação direta a tais instrumentos. Diante dessa lacuna regulatória parcial, impõe-se recorrer aos princípios gerais do Direito Civil, notadamente à boa-fé objetiva, à função social do contrato e aos critérios de interpretação contratual como parâmetros aptos a limitar e controlar os efeitos do automatismo, sem que isso implique negar a validade ou a utilidade econômica dessas tecnologias.

3.4 Síntese do raciocínio dedutivo

O raciocínio desenvolvido nesta seção estrutura-se de forma dedutiva, parte-se da premissa normativa geral segundo a qual aquele que exerce atividade que, por sua natureza, implique risco para os direitos de outrem responde objetivamente pelos danos causados, independentemente de culpa, conforme dispõe o art. 927, parágrafo único, do Código Civil.

Em seguida, formula-se a premissa fática: a automação contratual por meio de *smart contracts* pode, em determinadas configurações, potencializar danos em larga escala, dificultar a reversibilidade dos efeitos produzidos e ampliar assimetrias informacionais entre os participantes da relação jurídica.

A partir dessas premissas, sustenta-se construção argumentativa plausível segundo a qual os *smart contracts*, quando inseridos em contextos de elevada complexidade técnica e relevância econômica, podem ser enquadrados, em determinadas circunstâncias, como atividade de risco, atraindo a incidência da responsabilidade civil objetiva. Esse enquadramento não é tese pacífica na doutrina, mas encontra suporte em critérios objetivos verificáveis: (i) a escala potencial de dano, decorrente da capacidade de afetação automatizada e simultânea de múltiplos sujeitos; (ii) a irreversibilidade prática da execução, em arquiteturas estritamente imutáveis; e (iii) a assimetria informacional relevante entre desenvolvedores, plataformas e

usuários afetados. Trata-se, portanto, de conclusão dogmaticamente consistente no plano da hipótese, ainda que sujeita a divergências interpretativas.

Como conclusão parcial e atendendo ao objetivo específico (i) na dimensão da imputação, sustenta-se que o art. 927, parágrafo único, do Código Civil oferece base normativa suficiente para a responsabilização das plataformas digitais que utilizam *smart contracts* em contextos qualificados como atividade de risco, sem necessidade de criação de regime especial.

4 MITIGAÇÃO TÉCNICO-JURÍDICA: O TRIPÉ CORPORATIVO DE CONFORMIDADE APLICADO AOS *SMART CONTRACTS*

Qualquer discussão sobre padrões técnicos passa, antes, por uma pergunta fundamental: ‘quais valores guiarão a concepção da inovação?’ Para Pinheiro (PINHEIRO, 2024), o risco ético é o primeiro e mais urgente dos riscos a ser enfrentado.

Esse desafio encontra resposta concreta no tripé formado pelos Departamentos de *Compliance*, Auditoria e Segurança da Informação. Ao *Compliance* incumbe traduzir os valores pactuados em políticas internas, códigos de conduta e controles preventivos; à Auditoria, verificar, de modo independente e periódico, a aderência da organização a esses parâmetros; e à Segurança da Informação, blindar tecnicamente a integridade dos sistemas, evitando que falhas de segurança convertam riscos éticos latentes em danos jurídicos efetivos. O resultado dessa articulação é uma governança estruturada em camadas: a ética sai do papel e passa a ter função prática, capaz de atuar antes que o risco se concretize. Tais estruturas corporativas tendem a ser intrínsecas a organizações maduras, e seu funcionamento adequado contribui significativamente para a mitigação de riscos.

Campos e Carreiro (CAMPOS; CARREIRO, 2024) demonstram que a evolução dos programas de *Compliance* e gestão de riscos reflete a necessidade de adaptabilidade no cenário empresarial contemporâneo, impulsionada pela constante disrupção tecnológica, constatação que se torna ainda mais premente quando o objeto de regulação é, ele próprio, uma inovação disruptiva como os *smart contracts*. Nessa direção, estudos da Universidade Federal de Minas Gerais indicam que, embora os *smart contracts* sejam focados na *performance*, a noção de conformidade tratada por área de natureza técnico-jurídica composta por especialistas em tecnologia e em direito torna-se essencial para prevenir a materialização de riscos inerentes à automatização de obrigações (UNIVERSIDADE FEDERAL DE MINAS GERAIS, 2021).

Ao lado do *Compliance*, a Auditoria exerce função igualmente decisiva no enfrentamento dos riscos associados aos *smart contracts*, ao operar como instância

independente de verificação da conformidade entre o comportamento programado e os parâmetros jurídicos, técnicos e éticos previamente pactuados.

Nesse particular, Oliveira Farias et al. (2023) destacam que a própria arquitetura da tecnologia *blockchain* marcada por imutabilidade, rastreabilidade e registro descentralizado reconfigura o exercício da função auditora, possibilitando a transição de uma auditoria periódica e retrospectiva para um modelo de auditoria contínua, no qual cada transação pode ser verificada em tempo real. Essa transição não dispensa, mas exige, a auditoria especializada do próprio código-fonte dos *smart contracts*, porquanto, uma vez implantados, eventuais falhas lógicas ou vulnerabilidades tendem a ser, em regra, de difícil reversão, dada a limitação prática de alteração unilateral do registro distribuído.

Complementarmente, a área de Segurança da Informação (*Information Security*) constitui o terceiro pilar desse tripé preventivo, atuando sobre a dimensão técnica das vulnerabilidades que podem se converter em danos jurídicos concretos. O que se observa é que a implementação de *smart contracts* em plataformas digitais, embora promova ganhos de eficiência e automação contratual, carrega consigo um espectro de vulnerabilidades técnicas que, sem a devida governança, podem converter-se em riscos concretos.

A literatura especializada, a exemplo do levantamento sistemático conduzido por Atzei; Bartoletti; Cimoli (ATZEI; BARTOLETTI; CIMOLI, 2017), catalogou extenso rol de vetores de ataque específicos a *smart contracts* implantados em plataformas como a *Ethereum*, evidenciando que a mera execução correta do código é condição necessária, porém insuficiente, para assegurar a integridade das operações, o que torna recomendável a incorporação de auditorias de código e mecanismos de verificação formal.

Na mesma direção, De Filippi; Wright (DE FILIPPI; WRIGHT, 2018) e Rahman (RAHMAN, 2025) apontam que a natureza transfronteiriça e descentralizada dos *smart contracts* agrava o cenário de risco, na medida em que a fragmentação regulatória entre jurisdições gera lacunas normativas que favorecem a materialização de violações legais. Segundo esses autores, somente procedimentos que incorporem requisitos de identificação tendem a se mostrar capazes de preencher essas lacunas e conferir segurança jurídica às transações automatizadas.

A literatura nacional aponta na mesma direção, reconhecendo esses departamentos como pilares centrais de conformidade nas plataformas que operam com contratos inteligentes. Ricardo (RICARDO, 2026) ao investigar a governança de criptoativos no contexto da prevenção a ilícitos financeiros, sustenta que o monitoramento automatizado via *smart contracts* constitui ferramenta preventiva relevante, mas que se revela insuficiente sem a

adequação concomitante a marcos normativos globais, evidenciando a necessidade de camadas institucionais de Conformidade que transcendam a automação puramente tecnológica.

Quando o algoritmo passa a produzir decisões cuja explicação escapa à compreensão imediata, inclusive de seus próprios programadores, tende-se a atribuir-lhe uma função que extrapola a verificação de conformidade interna, podendo assumir relevância na construção do acervo probatório. Korkmaz (KORKMAZ, 2024) mostra que o uso de *machine learning* e redes neurais aprofunda esse problema, tornando a demonstração do nexo causal entre a falha algorítmica e o dano sofrido um desafio simultaneamente técnico e jurídico. Por isso, os registros produzidos pelos programas de conformidade, relatórios de impacto, atas, documentação de testes e registros de monitoramento, tendem a constituir importante acervo probatório disponível ao julgador para avaliar a diligência da plataforma. Em outras palavras: a atuação desses três departamentos e o acervo documental por eles produzido tendem a se mostrar elemento relevante para a distribuição do ônus probatório e para a eventual configuração ou afastamento do dever de indenizar.

Vale destacar, ainda, que a automação de obrigações jurídicas por meio de *smart contracts* não isenta as plataformas digitais do dever de diligência que permeia todo o ordenamento civil brasileiro; ao contrário, a natureza autoexecutável desses instrumentos tende a intensificar esse dever, tornando ainda mais exigível a articulação coordenada entre as três esferas examinadas. Erros de programação, cláusulas abusivas ou falhas algorítmicas produzem efeitos imediatos e, em regra, de difícil remediação sobre as partes.

É previsível que a ausência ou a fragilidade de qualquer desses três pilares *Compliance*, Auditoria e Segurança da Informação comprometa a governança dos *smart contracts* nas plataformas digitais e potencialize a materialização de danos patrimoniais e violações aos direitos da personalidade. A atuação coordenada desses departamentos não se apresenta como mera recomendação de boas práticas corporativas, mas como condição de diligência juridicamente exigível das plataformas, cuja observância ou inobservância tende a influenciar de modo relevante o juízo de responsabilidade civil. Nesse sentido, como conclusão parcial e em atendimento ao objetivo específico (i), sustenta-se que tais estruturas tendem a mitigar a materialização de riscos associados à automação contratual, assumindo relevância tanto para a aferição do dever de diligência quanto para a definição da distribuição do ônus probatório.

Cabe notar que a assimetria de custos exige que o rigor regulatório seja calibrado pela proporcionalidade, evitando que o ônus da conformidade sufoque agentes de menor porte.

Essa lógica escalonada, presente no *AI Act* e no PL nº 2.338/2023, tende a assegurar que as obrigações acompanhem a capacidade econômica e o grau de risco de cada plataforma.

5 CONCLUSÃO

O presente artigo partiu da problemática acerca de em que medida o ordenamento jurídico brasileiro dispõe de instrumentos normativos aptos a fundamentar a imputação de responsabilidade civil pelos danos decorrentes da execução automatizada de *smart contracts*, diante da inexistência de regulação específica e da complexidade técnica que marca a demonstração do nexo causal nesses contextos. A investigação desenvolvida permite sustentar resposta positiva, ainda que condicionada a relevantes ressalvas de ordem dogmática e prática.

A partir de raciocínio dedutivo, que tomou como premissas normativas gerais o sistema da responsabilidade civil, em especial o art. 927, parágrafo único, do Código Civil, verificou-se que o ordenamento jurídico brasileiro consagra orientação protetiva da parte vulnerável, extraível do Código Civil, do Código de Defesa do Consumidor e da Lei Geral de Proteção de Dados. Essa diretriz, embora construída em contextos anteriores à disseminação da automação contratual, pode ser estendida aos *smart contracts*, desde que interpretada à luz de suas especificidades técnicas e funcionais.

Nesse cenário, o principal desafio identificado não reside propriamente na inexistência de normas jurídicas aplicáveis, mas na dificuldade prática de acessar e reconstruir os eventos ocorridos no interior de sistemas automatizados e, em determinados casos, tecnicamente opacos. É nesse ponto que o tripé formado pelos Programas de Conformidade assume função decisiva, na medida em que tende a produzir registros, *logs*, relatórios e trilhas de auditoria capazes de funcionar como ponte probatória entre o comportamento do sistema e o dano alegado, contribuindo para a adequada distribuição do ônus da prova.

A elevada complexidade do código, associada às restrições à intervenção *ex post* em determinadas arquiteturas, faz com que a comprovação do nexo causal frequentemente dependa de perícia técnica especializada, a qual, na prática, pode revelar-se inacessível ao sujeito hipossuficiente. Ausentes mecanismos jurídicos de redistribuição ou flexibilização do ônus probatório, a tutela do direito material tende a esvaziar-se no plano efetivo. É nesse cenário que o Projeto de Lei nº 2.338/2023, aprovado pelo Senado Federal em dezembro de 2024, assume especial relevância, ao prever, em seus arts. 35 a 37, a possibilidade de inversão do ônus da prova em favor da vítima hipossuficiente ou quando as características do sistema tornarem excessivamente onerosa a demonstração dos pressupostos da responsabilidade civil,

consolidando orientação já identificável no ordenamento jurídico, e não criando regime absolutamente inovador.

Como limitação da pesquisa, reconhece-se o recorte estritamente dogmático adotado, que não abrange análise empírica nem estudos aprofundados de impacto regulatório ou econômico, campos que demandariam metodologia distinta, de natureza interdisciplinar. Reconhece-se, ainda, que o estudo não esgota o tratamento das múltiplas variantes técnicas dos *smart contracts*, concentrando-se em sua configuração típica e em sua interação com plataformas digitais de trabalho.

Ainda assim, a principal contribuição científica do trabalho consiste em demonstrar, mediante encadeamento dedutivo articulado, que o Direito Civil brasileiro dispõe de mecanismos normativos suficientemente flexíveis para enfrentar os riscos jurídicos associados aos *smart contracts*, desde que interpretados de forma sistemática, prudente e funcional, e acompanhados de estruturas organizacionais eficazes de governança tecnológica. Tal abordagem tende a permitir a conciliação entre a proteção dos direitos fundamentais e a preservação da inovação, evitando tanto o vácuo normativo quanto soluções de responsabilização excessiva capazes de comprometer o desenvolvimento tecnológico.

Embora a expansão da responsabilidade civil nos *smart contracts* seja debatida, parte da doutrina alerta que o rigor excessivo pode inflar os custos dos Programas de Conformidade e sufocar a inovação de pequenos agentes econômicos. Por outro lado, regimes demasiadamente permissivos tendem a externalizar os custos do risco para usuários em posições mais vulneráveis. O equilíbrio regulatório, portanto, exige avaliação contextual e proporcional, atenta à graduação do risco, às possibilidades técnicas de mitigação e à adequada distribuição dos benefícios e ônus da inovação, tarefa que, no contexto brasileiro, ainda carece de sedimentação normativa específica no tocante aos *smart contracts*.

Em um paralelo final, a investigação oferece elementos que sustentam a hipótese inicialmente proposta, indicando que o ordenamento jurídico brasileiro dispõe de bases normativas suscetíveis de fundamentar, em determinadas hipóteses, a responsabilização das plataformas digitais que utilizam *smart contracts*, desde que submetidas a interpretação sistemática e articuladas com mecanismos preventivos e probatórios de governança tecnológica. A afirmação dessa leitura, entretanto, permanece condicionada ao avanço da disciplina legislativa específica e ao amadurecimento da construção jurisprudencial, em especial no tocante à prova do nexo causal e à adequada distribuição do ônus probatório.

REFERÊNCIAS

ATZEI, Nicola; BARTOLETTI, Massimo; CIMOLI, Tiziana. A survey of attacks on Ethereum smart contracts (SoK). In: MAFFEI, Matteo; RYAN, Mark (ed.). Principles of Security and Trust. POST 2017. (Lecture Notes in Computer Science, v. 10204). Berlin: Springer, 2017. p. 164-186. Disponível em: https://doi.org/10.1007/978-3-662-54455-6_8. Acesso em: 16 abr. 2026.

BARBOSA, Mafalda Miranda. IA, riscos e responsabilidade: uma reflexão em torno do Regulamento IA e do Projeto de Lei brasileiro nº 2.338, de 2023. Revista Brasileira de Direito Civil – RBDCivil, Belo Horizonte, v. 33, n. 4, p. 163-189, out./dez. 2024.

BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília: Presidência da República, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 19 abr. 2026.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Código de Defesa do Consumidor. Brasília: Presidência da República, 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/18078.htm. Acesso em: 19 abr. 2026.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Brasília: Presidência da República, 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/110406.htm. Acesso em: 19 abr. 2026.

BRASIL. Lei nº 12.414, de 9 de junho de 2011. Lei do Cadastro Positivo. Brasília: Presidência da República, 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/112414.htm. Acesso em: 19 abr. 2026.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em: 19 abr. 2026.

BRASIL. Senado Federal. Projeto de Lei nº 2.338, de 2023. Dispõe sobre o uso da Inteligência Artificial. Brasília: Senado Federal, 2023. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/157233>. Acesso em: 19 abr. 2026.

BRASIL. Tribunal Superior do Trabalho. Informativo TST nº 291 (19 a 31 de agosto de 2024). Brasília: TST/CJUR, 2024. Disponível em: <https://www.tst.jus.br/web/guest/informativos>. Acesso em: 19 abr. 2026.

CAMPOS, Rafael; CARREIRO, Marcelo. Compliance e gestão de riscos em tempos de inovação e disrupção digital. Revista de Gestão e Secretariado, v. 15, n. 4, 2024. Disponível em: <https://doi.org/10.7769/gesec.v15i4.3743>. Acesso em: 16 abr. 2026.

CASTELLS, Manuel. A sociedade em rede. Tradução de Roneide Venancio Majer. 8. ed. São Paulo: Paz e Terra, 2005.

DE FILIPPI, Primavera; WRIGHT, Aaron. Blockchain and the Law: the rule of code. Cambridge: Harvard University Press, 2018.

FEFERBAUM, Marina; QUEIROZ, Rafael Mafei Rabelo (org.). Metodologia da pesquisa em direito: técnicas e abordagens para elaboração de monografias, dissertações e teses. 2. ed. São Paulo: Saraiva, 2019.

KORKMAZ, Maria Regina Rigolon. Decisões automatizadas: explicação, revisão e proteção na era da inteligência artificial. São Paulo: Revista dos Tribunais, 2024.

LEMOS, André. Cibercultura: tecnologia e vida social na cultura contemporânea. 9. ed. Porto Alegre: Sulina, 2023.

LÉVY, Pierre. As tecnologias da inteligência: o futuro do pensamento na era da informática. Rio de Janeiro: Editora 34, 1993.

NAKAMOTO, Satoshi. Bitcoin: a peer-to-peer electronic cash system. [S. l.: s. n.], 2008. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 19 abr. 2026.

NETA, Ainah Hohenfeld Angelini; NUNES, Lorena de Almeida. Marco regulatório da inteligência artificial: análise do AI Act da União Europeia no tocante à privacidade e proteção dos dados pessoais. Revista de Direito da UNIFACS, 2024. Disponível em: <https://revistas.unifacs.br/index.php/redu/article/viewFile/9279/5266>. Acesso em: 19 abr. 2026.

OLIVEIRA FARIAS, Diego; TEIXEIRA COUTINHO, Eldon; MONTEIRO, Monique; CESAR JOCUNDO LOUREIRO, Tibério. Tecnologia Blockchain e auditoria. Revista do TCU, Brasília, v. 150, n. 150, p. 22-48, 2023. Disponível em: <https://revista.tcu.gov.br/ojs/index.php/RTCU/article/view/1921>. Acesso em: 19 abr. 2026.

PINHEIRO, Patricia Peck Garrido (coord.). Direito Digital Aplicado 6.0. São Paulo: Revista dos Tribunais, 2024.

RAHMAN, Samiur. Standardizing smart contracts for regulatory compliance in cross-border payments. International Journal of Law, Social Science, and Humanities, v. 2, n. 3, p. 295-306, 2025. Disponível em: <https://doi.org/10.70193/ijlsh.v2i3.260>. Acesso em: 16 abr. 2026.

RICARDO, Jaison Sfogia. Governança de criptoativos e compliance regulatório: desafios globais na prevenção de ilícitos financeiros digitais. Revista Ibero-Americana de Humanidades, Ciências e Educação, v. 12, n. 1, p. 1-24, jan. 2026. Disponível em: <https://doi.org/10.51891/rease.v12i1.20387>. Acesso em: 16 abr. 2026.

SZABO, Nick. Smart contracts. 1994. Disponível em: <https://nakamotoinstitute.org/library/smart-contracts/>. Acesso em: 19 abr. 2026.

SZABO, Nick. Smart contracts: building blocks for digital markets. 1996. Disponível em: <https://nakamotoinstitute.org/library/smart-contracts-building-blocks-for-digital-markets/>. Acesso em: 19 abr. 2026.

TEPEDINO, Gustavo; SILVA, Rodrigo da Guia. Inteligência artificial e elementos da responsabilidade civil. In: FRAZÃO, Ana; MULHOLLAND, Caitlin (coord.). Inteligência artificial e direito: ética, regulação e responsabilidade. 2. ed. rev., atual. e ampl. São Paulo: Revista dos Tribunais, 2020.

UNIÃO EUROPEIA. Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024 (Artificial Intelligence Act). Jornal Oficial da União Europeia, L, 2024. Disponível em: <https://eur-lex.europa.eu>. Acesso em: 19 abr. 2026.

UNIVERSIDADE FEDERAL DE MINAS GERAIS. Direito e tecnologia: novos modelos e tendências. Belo Horizonte: PPGD/UFGM, 2021. Disponível em: <https://pos.direito.ufmg.br/downloads/079-Direito-e-Tecnologia-1-1.pdf>. Acesso em: 15 abr. 2026.

WERTHEIN, Jorge. A sociedade da informação e seus desafios. *Ciência da Informação*, Brasília, v. 29, n. 2, p. 71-77, maio/ago. 2000. Disponível em: <http://revista.ibict.br/ciinf/article/view/2337>. Acesso em: 19 abr. 2026.