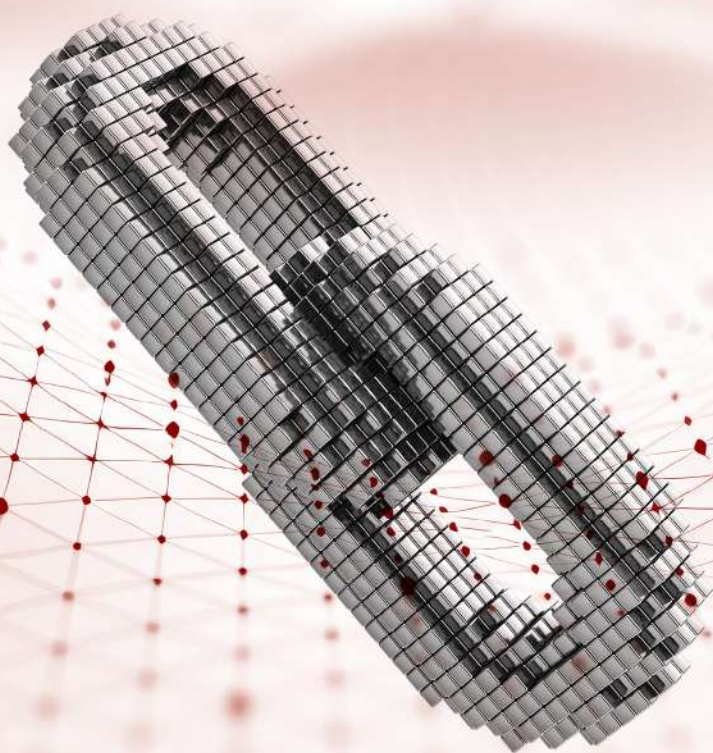


(Organizador)
José Luiz de Moura Faleiros Júnior

DIREITO, BLOCKCHAIN

e governança de dados



A obra reúne estudos que examinam os impactos jurídicos das tecnologias emergentes sobre contratos, mercados, políticas públicas, estruturas regulatórias e direitos fundamentais, percorrendo temas como contratos algorítmicos, smart contracts, criptoativos, tokenização, proteção de dados, cidades inteligentes, inteligência artificial, segurança pública e inovação no setor estatal. Trata-se de uma leitura destinada a pesquisadores, profissionais e estudantes interessados em compreender, com profundidade crítica, algumas das principais questões jurídicas da sociedade digital contemporânea.

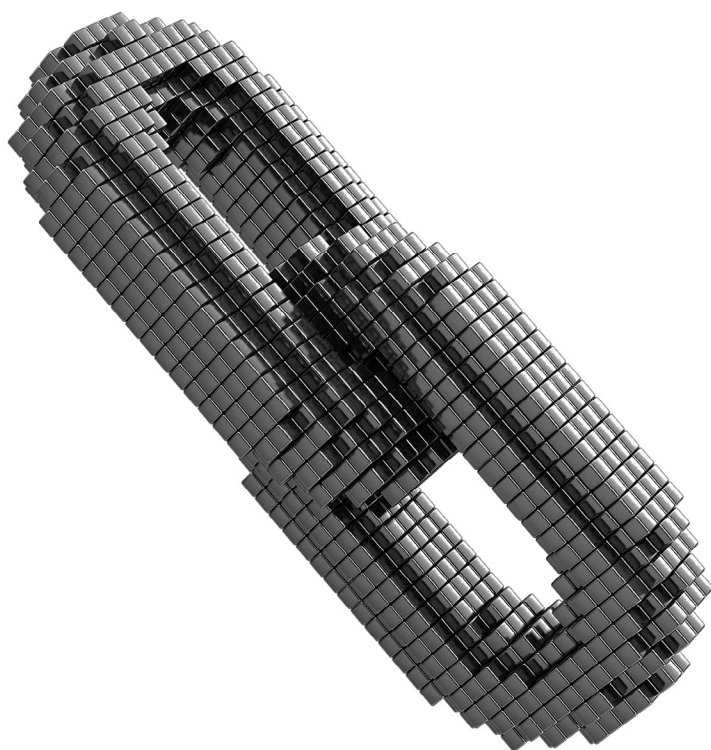
ISBN 978-65-6006-317-4



9 786560 063174 >

DIREITO, BLOCKCHAIN

e governança de dados



Direção Executiva: Luciana de Castro Bastos
Direção Editorial: Daniel Carvalho
Diagramação e Capa: Editora Expert
A regra ortográfica usada foi prerrogativa do autor



Todos os livros publicados pela Expert Editora Digital estão sob os direitos da Creative Commons 4.0 BY-SA. <https://br.creativecommons.org/>
"A prerrogativa da licença creative commons 4.0, referencias, bem como a obra, são de responsabilidade exclusiva do autor"

A Expert Editora, bem como a organização da obra não se responsabilizam por quaisquer posições, opiniões e condutas compartilhadas nesta obra, sendo o conteúdo dos capítulos de responsabilidade exclusiva de seus respectivos autores.

Dados Internacionais de Catalogação na Publicação (CIP)

F187d Faleiros Júnior, José Luiz de Moura (organizador)
Direito, blockchain e governança de dados / José Luiz de Moura Faleiros Júnior (organizador). – Belo Horizonte : Expert Editora Digital, 2026.
422 p.

ISBN: 978-65-6006-317-4

Modo de acesso: <https://experteditora.com.br>

1. Direito digital. 2. Blockchain. 3. Proteção de dados. 4. Criptoativos. 5. Governança de dados. 6. Inteligência artificial. I. Faleiros Júnior, José Luiz de Moura, org.
II. Título.

CDD: 340.0285

CDU: 34:004

Índices para catálogo sistemático:

Direito digital / Direito e tecnologia – CDD 340.0285 / CDU 34:004

experteditora.com.br
contato@editoraexpert.com.br





Prof. Dra. Adriana Goulart De Sena Orsini

Universidade Federal de Minas Gerais - UFMG

**Prof. Dr. Alexandre Miguel
Cavaco Picanco Mestre**

Universidade Autónoma de Lisboa, Escola.
Superior de Desporto de Rio Maior, Escola.
Superior de Comunicação Social (Portugal),
The Football Business Academy (Suíça)

Prof. Dra. Amanda Flavio de Oliveira

Universidade de Brasília - UnB

Prof. Dr. Carlos Raul Iparraguirre

Facultad de Ciencias Jurídicas y Sociales,
Universidad Nacional del Litoral (Argentina)

Prof. Dr. César Mauricio Giraldo

Universidad de los Andes, ISDE, Universidad
Pontificia Bolivariana UPB (Bolívia)

Prof. Dr. Eduardo Goulart Pimenta

Universidade Federal de Minas Gerais - UFMG.
e PUC - Minas

Prof. Dr. Gladston Mamede

Advogado e escritor

Prof. Dr. Francisco Satiro

Faculdade de Direito da USP - Largo São
Francisco

Prof. Dr. Gustavo Lopes Pires de Souza

Universidad de Litoral (Argentina)

Prof. Dr. Henrique Viana Pereira

PUC - Minas

Prof. Dr. Javier Avilez Martínez

Universidad Anahuac, Universidad
Tecnológica de México (UNITEC), Universidad
Del Valle de México (UVM) (México)

Prof. Dr. João Bosco Leopoldino da Fonseca

Universidade Federal de Minas Gerais - UFMG.

Prof. Dr. Julio Cesar de Sá da Rocha

Universidade Federal da Bahia - UFBA

Prof. Dr. Leonardo Gomes de Aquino

UnICEUB e UniEuro, Brasília, DF.

Prof. Dr. Leonardo Ferreira Vilaça

Universidade de Itaúna - UIT e Universidade
do Estado de Minas Gerais - UEM

Prof. Dr. Luciano Timm

Fundação Getúlio Vargas - FGVSP

Prof. Dr. Mário Freud

Faculdade de direito Universidade
Agostinho Neto (Angola)

Prof. Dr. Marcelo Andrade Féres

Universidade Federal de Minas Gerais - UFMG

Prof. Dr. Omar Jesús Galarreta Zegarra

Universidad Continental sede Huancayo,
Universidad Sagrado Corazón (UNIFE),
Universidad Cesar Vallejo. Lima Norte (Peru)

Prof. Dr. Rafael Soares Duarte de Moura

Universidade Estadual De Montes Claros

Prof. Dr. Raphael Silva Rodrigues

Centro Universitário Unihorizontes
e Universidade Federal de Minas Gerais - UFMG

Prof. Dra. Renata C. Vieira Maia

Universidade Federal de Minas Gerais - UFMG

Prof. Dr. Rodolpho Barreto Sampaio Júnior

PUC - Minas e Faculdade Milton Campos

Prof. Dr. Rodrigo Almeida Magalhães

Universidade Federal de Minas Gerais - UFMG.
PUC - Minas

Prof. Dr. Thiago Penido Martins

Universidade do Estado de
Minas Gerais - UEMG

AGRADECIMENTOS

Esta obra é fruto das pesquisas desenvolvidas no Instituto de Tecnologia e Sociedade do Rio de Janeiro – ITS Rio, a partir das investigações realizadas pelos discentes do curso de Pós-Graduação em Direito Digital nos anos de 2025 e 2026. Cada capítulo representa o resultado de um percurso acadêmico marcado pelo estudo atento, pelo amadurecimento crítico e pelo compromisso de compreender, sob diferentes perspectivas, os impactos jurídicos produzidos pelas tecnologias emergentes.

Registro, inicialmente, meu profundo agradecimento ao ITS Rio, instituição que se destaca pela excelência de suas atividades acadêmicas e por sua contribuição permanente para o desenvolvimento do Direito Digital no Brasil. O ambiente de liberdade intelectual, diálogo interdisciplinar e abertura à inovação proporcionado pelo Instituto foi essencial para que as pesquisas reunidas neste livro pudessem ser concebidas, desenvolvidas e aperfeiçoadas.

Agradeço, de modo muito especial, aos autores e autoras desta coletânea, que se dedicaram com seriedade e entusiasmo às investigações que deram origem aos capítulos aqui publicados. A diversidade dos temas abordados e a qualidade das reflexões apresentadas revelam não apenas o empenho individual de cada pesquisador, mas também a riqueza das discussões promovidas ao longo do curso. Organizar esta obra e acompanhar o desenvolvimento desses trabalhos constituiu, para mim, uma experiência acadêmica especialmente gratificante.

Estendo meus agradecimentos aos professores, pesquisadores, profissionais e colaboradores que, direta ou indiretamente, contribuíram para a formação dos discentes e para o ambiente intelectual no qual estas pesquisas foram realizadas. A produção científica é sempre resultado de uma construção coletiva, alimentada pelo diálogo, pelo intercâmbio de ideias e pela disposição de revisar certezas diante dos novos desafios impostos pela realidade.

Agradeço também à Editora Expert pela confiança depositada neste projeto, pelo acolhimento da proposta editorial e pelo cuidado dedicado à publicação da obra. A parceria com uma editora comprometida com a difusão do conhecimento jurídico e com a valorização da produção acadêmica é motivo de especial satisfação.

Por fim, agradeço aos leitores que se dispõem a percorrer estas páginas. É na leitura, no debate e na crítica que a pesquisa acadêmica encontra sua verdadeira continuidade. Espero que os estudos reunidos nesta coletânea contribuam para novas reflexões, estimulem outras investigações e auxiliem na construção de respostas juridicamente consistentes, socialmente responsáveis e tecnicamente adequadas aos desafios da inovação.

A todos que tornaram possível a realização deste livro, registro minha sincera gratidão.

APRESENTAÇÃO

A obra coletiva “Direito, *blockchain* e governança de dados” reúne estudos que examinam como tecnologias emergentes vêm alterando categorias tradicionais do Direito, estruturas de mercado, políticas públicas e mecanismos de proteção de direitos fundamentais. Os capítulos articulam perspectivas de Direito Civil, Empresarial, Tributário, Processual, Administrativo, Regulatório e de Proteção de Dados, tendo como elemento comum a necessidade de conciliar inovação, segurança jurídica, governança e responsabilidade. O propósito da coletânea é oferecer ao leitor um panorama plural e aplicado dos desafios jurídicos decorrentes da incorporação de *blockchain*, criptoativos, sistemas algorítmicos e modelos intensivos em dados por agentes privados e pelo Poder Público.

O Capítulo 1, de minha autoria, investiga os contratos algorítmicos executados em *blockchain* e as tensões entre a rigidez do código e a teoria da onerosidade excessiva. O estudo distingue contratos eletrônicos, contratos inteligentes e contratos algorítmicos, demonstrando que a autoexecutoriedade não elimina a incidência dos princípios contratuais. Nesse contexto, examina os chamados *circuit breakers* como mecanismos capazes de interromper temporariamente a execução automatizada diante de eventos extraordinários, sem substituir a necessária avaliação jurídica e humana do desequilíbrio superveniente.

O Capítulo 2, de Manuela Machado Gonçalves, examina a aplicação dos smart contracts à gestão e à distribuição de direitos autorais nos mercados musical e audiovisual. A autora compara o modelo de arrecadação e distribuição do ECAD com as práticas contratuais do setor audiovisual, marcadas pela recorrência de pagamentos únicos e cláusulas de buyout, e investiga como infraestruturas baseadas em *blockchain* podem reduzir assimetrias informacionais, automatizar a divisão de royalties e ampliar a rastreabilidade dos fluxos financeiros. O estudo também aborda os smart legal contracts, a governança de dados, o papel dos oráculos, experiências como a FilmChain e os

Royalty Splits e os desafios regulatórios, técnicos e de proteção de dados envolvidos na adoção dessas soluções no Brasil.

O Capítulo 3, de Davi Wainer Costa, analisa o conflito entre a imutabilidade dos registros em blockchain e os direitos assegurados pela legislação de proteção de dados pessoais, especialmente o direito de eliminação. O autor apresenta os fundamentos técnicos das redes distribuídas e avalia mecanismos criptográficos como armazenamento *off-chain*, rotação de chaves, *crypto-shredding*, criptografia homomórfica, provas de conhecimento zero, *pruning* e *chameleon hashes*. O capítulo demonstra que a conformidade não depende da supressão física absoluta dos registros, mas da adoção de soluções técnicas e de governança orientadas pelo *privacy by design*.

O Capítulo 4, de Karina Chagas dos Santos, examina a blockchain como investimento estratégico para o monitoramento da sustentabilidade em cadeias de suprimentos. A pesquisa relaciona imutabilidade, transparência e rastreabilidade à verificação de práticas empresariais e indicadores socioambientais, demonstrando como registros distribuídos podem aumentar a confiança entre fornecedores, empresas e consumidores. O estudo também pondera desafios regulatórios, econômicos e operacionais que condicionam a implementação responsável dessas soluções.

O Capítulo 5, de Julianna Ramalho Fonseca, apresenta uma análise abrangente dos impactos jurídicos e tributários dos criptoativos e da tokenização sobre a estrutura societária e comercial das empresas brasileiras. O texto percorre a classificação dos tokens, o Marco Legal dos Ativos Virtuais, a atuação da Comissão de Valores Mobiliários, do Banco Central e da Receita Federal, além dos desafios relacionados à integralização de capital, aos *smart contracts*, à tokenização de recebíveis e à tributação de operações realizadas no Brasil e no exterior. A autora destaca a necessidade de harmonização regulatória e modernização dos registros empresariais.

O Capítulo 6, de Matheus Silva Reis, aborda a tokenização de ativos como instrumento de democratização do acesso ao mercado de capitais brasileiro. O trabalho examina a infraestrutura formada

por blockchain e *smart contracts*, as barreiras históricas ao ingresso de investidores e as possibilidades abertas pelo fracionamento de ativos, pela redução de custos e pela diminuição da dependência de intermediários tradicionais. O capítulo também analisa os limites regulatórios relacionados à natureza jurídica dos tokens, à proteção do investidor, à prevenção à lavagem de dinheiro e à segurança das operações.

O Capítulo 7, de Larissa Celestino Teles, dedica-se à penhora de criptoativos no Brasil. A autora reconstrói conceitos relativos a moeda, criptomoedas, tokens, blockchain, tecnologias de registro distribuído e modalidades de custódia, para então examinar os obstáculos práticos à localização, ao bloqueio e à transferência judicial desses ativos. O texto destaca o papel das exchanges, as dificuldades criadas por carteiras autocustodiadas e a relevância de iniciativas tecnológicas e regulatórias, como o desenvolvimento de mecanismos de comunicação judicial especializados.

O Capítulo 8, de Luís Henrique de Menezes Acioly, relaciona a digitalização do registro de imóveis à implementação da agenda brasileira para cidades inteligentes. O estudo investiga a governança e a interoperabilidade dos dados imobiliários, o georreferenciamento e o potencial do Sistema de Registro Eletrônico de Imóveis para subsidiar políticas públicas municipais orientadas por evidências. Ao analisar instrumentos e atos normativos do Conselho Nacional de Justiça, o autor demonstra como informações registrais atualizadas podem contribuir para planejamento urbano, sustentabilidade e gestão territorial.

O Capítulo 9, de George José Nascimento de Souza, examina os sandboxes regulatórios como instrumentos de experimentação jurídica e tecnológica em cidades inteligentes, com especial atenção ao tratamento de dados pessoais. A partir do caso Recife Living Labs e de soluções de videovigilância inteligente, o capítulo discute bases legais, responsabilidade da Administração Pública, avaliação de impacto, minimização, transparência e supervisão contínua. O estudo propõe

salvaguardas para que ambientes experimentais promovam inovação sem reduzir o nível de proteção conferido aos titulares dos dados.

O Capítulo 10, de Desirée Marcelle da Cunha, analisa o uso da blockchain na prevenção de fraudes em contratações públicas à luz da Lei nº 14.133/2021. A autora identifica vulnerabilidades decorrentes de assimetrias informacionais, discricionariedade e opacidade procedimental e avalia como a imutabilidade, a rastreabilidade e a auditabilidade dos registros podem fortalecer transparência, governança e integridade. A pesquisa considera experiências nacionais e estrangeiras e sustenta a viabilidade de modelos permissionados ou híbridos compatíveis com o regime jurídico-administrativo brasileiro.

O Capítulo 11, de Felipe Tavares de Assis, aplica o conceito de metarregulação à análise da estratégia institucional da Agência Nacional de Proteção de Dados. O trabalho apresenta os fundamentos, riscos e limites da metarregulação, examina os instrumentos previstos na Lei Geral de Proteção de Dados e avalia o desenho institucional, a agenda regulatória, a fiscalização e a racionalidade responsiva da autoridade. Ao final, identifica limitações de capacidade, coerência e recursos, propondo parâmetros para o aprimoramento da atuação regulatória.

O Capítulo 12, de Giovanna de Amorim Freitas, investiga os efeitos da utilização de inteligência artificial na tomada de decisões empresariais sobre o dever de diligência dos administradores. A autora demonstra que a delegação de tarefas a sistemas algorítmicos não rompe a imputação jurídica das decisões, mas intensifica os deveres de informação, supervisão e controle. O capítulo também analisa discriminação algorítmica, vieses incorporados aos dados e ao design dos sistemas e a regulação baseada em risco como elemento de densificação dos padrões de governança corporativa.

O Capítulo 13, de Rafaela de Oliveira Lopes, encerra a obra com uma análise da Portaria MJSP nº 961/2025 e do emprego de tecnologias da informação em atividades de investigação criminal e inteligência de segurança pública. O estudo confronta ganhos de eficiência proporcionados por inteligência artificial, big data, reconhecimento

facial e análise preditiva com riscos à privacidade, à proteção de dados, à paridade de armas e às garantias constitucionais. A autora reconhece a relevância da portaria, mas aponta lacunas que reforçam a necessidade de legislação específica e de maior participação pública na construção dos parâmetros regulatórios.

É, portanto, com especial satisfação que apresento esta obra ao público e convido cada leitor a percorrer os capítulos que a compõem, certo de que as reflexões aqui reunidas poderão contribuir para uma compreensão mais crítica, responsável e propositiva das transformações promovidas pela blockchain, pela governança de dados e pela inteligência artificial. Mais do que oferecer respostas definitivas, o livro pretende estimular novas perguntas, aproximar diferentes campos do conhecimento jurídico e fomentar o diálogo entre academia, instituições públicas, mercado e sociedade. Espero que a leitura seja proveitosa e que os estudos desenvolvidos pelos autores sirvam de ponto de partida para novas pesquisas, debates e soluções comprometidas com uma inovação juridicamente segura, socialmente responsável e verdadeiramente orientada à promoção de direitos.

Belo Horizonte/MG, 4 de agosto de 2026.

José Luiz de Moura Faleiros Júnior

ORGANIZADOR

José Luiz de Moura Faleiros Júnior

AUTORES

José Luiz de Moura Faleiros Júnior

Manuela Machado Gonçalves

Davi Wainer Costa

Karina Chagas dos Santos

Julianna Ramalho Fonseca

Matheus Silva Reis

Larissa Celestino Teles

Luís Henrique de Menezes Acioly

George José Nascimento de Souza

Desirée Marcelle da Cunha

Felipe Tavares de Assis

Giovanna de Amorim Freitas

Rafaela de Oliveira Lopes

SUMÁRIO

PARTE I — BLOCKCHAIN: CONTRATOS, CONFORMIDADE E SUSTENTABILIDADE

- 1. “Circuit breakers” e contratos algorítmicos: oráculos, eventos extraordinários e onerosidade excessiva21**

José Luiz de Moura Faleiros Júnior

- 2. Smart contracts e direitos autorais 49**

Manuela Machado Gonçalves

- 3. Da inviabilidade técnica à conformidade regulatória: um estudo sobre blockchain e criptografia aplicada à proteção de dados pessoais 67**

Davi Wainer Costa

- 4. Blockchain como investimento estratégico para averiguação da sustentabilidade na cadeia de suprimentos.....103**

Karina Chagas dos Santos

PARTE II — CRIPTOATIVOS, TOKENIZAÇÃO E CIRCULAÇÃO ECONÔMICA

- 5. Criptoativos e tokenização: impactos jurídicos e tributários na estrutura societária e comercial das empresas no Brasil..... 123**

Julianna Ramalho Fonseca

- 6. A tokenização de ativos como instrumento de democratização do acesso aos investimentos no mercado de capitais brasileiro155**

Matheus Silva Reis

- 7. A penhora de criptoativos no Brasil.....185**

Larissa Celestino Teles

PARTE III — TRANSFORMAÇÃO DIGITAL DO ESTADO E INOVAÇÃO PÚBLICA

- 8.** Contributos da digitização do registro de imóveis para efetivação da agenda brasileira para cidades inteligentes: governança de dados e políticas georreferenciadas 241

Luís Henrique de Menezes Acioly

- 9.** Sandboxes regulatórios e a proteção dos dados pessoais obtidos em ambientes experimentais.....275

George José Nascimento de Souza

- 10.** O uso da tecnologia blockchain no combate à fraude nas contratações públicas à luz da Lei nº 14.133/2021309

Desirée Marcelle da Cunha

PARTE IV — GOVERNANÇA REGULATÓRIA, INTELIGÊNCIA ARTIFICIAL E DIREITOS FUNDAMENTAIS

- 11.** Metarregulação e estratégia regulatória da Agência Nacional de Proteção de Dados: experiências e desafios.....327

Felipe Tavares de Assis

- 12.** Dever de diligência de administradores e inteligência artificial: desafios da delegação de poder decisório aos algoritmos diante do risco de resultados discriminatórios 359

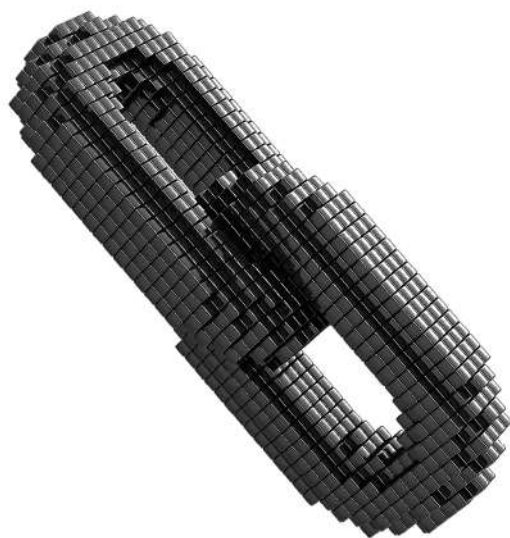
Giovanna de Amorim Freitas

- 13.** O equilíbrio delicado: a Portaria MJSP nº 961/2025 e a compatibilização entre o uso de tecnologia da informação na segurança pública e a proteção dos direitos fundamentais 393

Rafaela de Oliveira Lopes

PARTE I

BLOCKCHAIN: CONTRATOS,
CONFORMIDADE E SUSTENTABILIDADE



1. "CIRCUIT BREAKERS" E CONTRATOS ALGORÍTMICOS: ORÁCULOS, EVENTOS EXTRAORDINÁRIOS E ONEROSIDADE EXCESSIVA

José Luiz de Moura Faleiros Júnior

Doutor em Direito Civil pela Universidade de São Paulo (USP/Largo de São Francisco). Doutor em Direito, Tecnologia e Inovação pela Universidade Federal de Minas Gerais (UFMG). Mestre e Bacharel em Direito pela Universidade Federal de Uberlândia (UFU). Especialista em Direito Digital, Direito Civil e Empresarial. Advogado.

1 INTRODUÇÃO

A notável expansão dos protocolos de registro distribuído, conjugada ao emprego de algoritmos e modelos em sistemas de inteligência artificial na tessitura obrigacional, inaugurou cenário de contratualidade em que códigos imutáveis substituem a vigilância humana, exigindo revisão dogmática que reafirme o núcleo principiológico do direito civil, máxime a justiça contratual. Nesta senda, este artigo examina particularidades das contratações algorítmicas *onchain*, destacandolhe as tensões com a teoria da onerosidade excessiva, instituto consagrado pelos artigos 478 a 480 do Código Civil, recuperando a centralidade da boa-fé objetiva e da função social dos contratos.

Sabe-se que diversas investigações concernentes aos impactos e às limitações dos chamados contratos inteligentes (*smart contracts*), usualmente compreendidos, contemporaneamente, pela utilização da rede *blockchain* para sua instrumentalização, têm levado a discrepâncias sobre sua viabilidade jurídica ou, até mesmo, sobre a amplitude de seu conceito. A difusão das *blockchains* públicas, notadamente da Ethereum, materializou a promessa de autotutela digital, permitindo que cláusulas codificadas se autoexecutem sem interpelação judicial. Todavia, a rigidez determinística desses *scripts* inviabiliza a revisitação

do sinalagma diante de eventos extraordinários, incapazes de serem antecipados pelos programadores. Destarte, investigase a dicotomia entre segurança e flexibilidade, demonstrando que a onerosidade excessiva permanece elemento vital à justiça contratual e que, sem janelas de suspensão, o devedor pode ser coagido a sacrifício patrimonial desmesurado, contraditando a teleologia corretiva perseguida pelo ordenamento. É justamente nesse ponto que os *circuit breakers* se projetam como instrumentos de mitigação, permitindo, ao menos em tese, que o fluxo de autoexecutoriedade seja interrompido até que se avalie a extensão do desequilíbrio superveniente.

Sendo certo que algoritmos de inteligência artificial estão no cerne do desenvolvimento dessas tecnologias, o potencial disruptivo dessa transformação gera natural empolgação, mas institutos jurídicos tradicionais e que regem o direito dos contratos passam a ser contrastados aos desafios impostos pelas novas formas de instrumentalização da vontade. A ausência de permeabilidade desses scripts a eventos extraordinários demonstra, desde logo, a necessidade de repensar mecanismos que integrem prudência humana ao ciclo de execução, razão pela qual estruturas de interrupção emergencial, como os já mencionados *circuit breakers*, surgem como tentativa de compatibilização entre automação e justiça contratual.

Diferenças conceituais entre os contratos eletrônicos – estudados há tempos pela doutrina – e os contratos inteligentes (pouco utilizados, mas analisados, preponderantemente, no plano teórico) abrem margem a uma nova construção: a dos contratos algorítmicos, propostos originalmente por Lauren H. Scholz, e identificados pelas expressões inglesas *algorithmic contracts* e *self-driving contracts*. Referida terminologia permite categorizar mais adequadamente o tema, pois reflete com maior exatidão o estado da técnica no qual tais estruturas já se tornaram viáveis.

O tema-problema da pesquisa se situa justamente no contraponto à natural empolgação criada pela utilização dessas estruturas autodefinidas e autoexecutáveis frente a eventos de onerosidade excessiva, pois há consequências decorrentes da inflexibilidade, que já

foram apontadas pela doutrina – nomeadamente por Jeremy Sklaroff – no contexto dos *smart contracts* e da rede *blockchain*. A dúvida que paira, quanto à onerosidade excessiva, é se seus efeitos são os mesmos para os contratos algorítmicos autodefinidos¹.

Trabalhar-se-á com a hipótese de que o campo de aplicação dessas estruturas deve se restringir a situações mais singelas e menos propensas ao desequilíbrio, sob pena de sua inflexibilidade provocar distorções evitáveis e previsíveis, não pela natureza do negócio jurídico, mas pela forma adotada no pacto. Noutros termos, buscar-se-á, a partir do esclarecimento das citadas categorias conceituais, apontar a incompatibilidade atual da teoria da onerosidade excessiva com os modelos contratuais algorítmicos.

A distinção terminológica adotada — substituição do rótulo “*smart contract*” por “contrato algorítmico *onchain*” — desmistifica a falsa conotação de inteligência. A *blockchain* concede hígidez, não raciocínio; o termo corrige equívocos, estabelecendo premissa conceitual rigorosa para debates dogmáticos, evitando confusões entre autoexecução e autoadaptação. Tal precisão propicia análise mais fina da incidência da onerosidade excessiva, pois evidencia que a causa do desequilíbrio não jaz na tecnologia subjacente, mas na impermeabilidade do código ao diálogo hermenêutico. Nesse panorama, mecanismos como os *circuit breakers* funcionam apenas como paliativos técnicos, incapazes de substituir a ponderação judicial ou a renegociação humana.

Adotase metodologia dogmática, cotejando dispositivos centrais do Código Civil com achados da literatura estrangeira sobre *algorithmic governance*; partese da concepção de contratos algorítmicos *onchain* enquanto códigos imutáveis gravados em *ledger* distribuído, contrapondoos aos contratos eletrônicos convencionais, cuja execução permanece elástica.

1 FALEIROS JÚNIOR, José Luiz de Moura. Contratos algorítmicos e onerosidade excessiva: as consequências da inflexibilidade. *Civilistica.com - Revista Eletrônica de Direito Civil*, Rio de Janeiro, v. 11, p. 1-13, 2022, p. 4.

2 CONTRATOS ELETRÔNICOS, INTELIGENTES E ALGORÍTMICOS: QUAIS SÃO SUAS DIFERENÇAS?

Os contratos eletrônicos remontam às primeiras trocas comerciais mediadas por redes telemáticas, nas quais a manifestação de vontade se formaliza por cliques, assinaturas digitais ou correio eletrônico, mantendo, contudo, estrutura dogmática idêntica ao contrato escrito tradicional. Sua execução conserva margem ampla para renegociações, resilições e ajustes, pois a etapa de cumprimento ainda se processa no domínio sociotécnico, não sendo rigidamente vinculada a condições programadas irreversíveis. A jurisprudência brasileira reconhece-os como negócios jurídicos válidos desde que preservem consentimento informado, objeto lícito e forma livre, sujeitando-os integralmente ao regime geral do Código Civil, inclusive quanto à possibilidade de revisão.

A instrumentalização da vontade por meio eletrônico não é tema novo na disciplina jurídica dos contratos. Com a popularização dos microcomputadores e da Internet, na década de 1990, a doutrina se dedicou a estudar o tema e, na época, falava-se em contratos informáticos, virtuais, telemáticos, via Internet, dentre tantas outras designações.² Os problemas, porém, não eram apenas terminológicos: havia grande dificuldade de se compreender a extensão ultrafronteiriça³ da Internet e os inegáveis impactos que representou, desde sua

2 DE LUCCA, Newton. *Aspectos jurídicos da contratação informática e telemática*. São Paulo: Saraiva, 2003, p. 20. Anota, elucidando até mesmo a terminologia originalmente utilizada na Itália, na França e na Espanha: “Na doutrina peninsular, por exemplo, pelo genérico nome de *contratti d’informatica* são designados tanto os *contratti di utilizzazione del computer* – nos quais os bens ou serviços informáticos constituem o objeto do contrato – quanto os *contratti informatici*, vale dizer, aqueles em que a informática constitui um meio de representação ou de expressão da vontade, o mesmo acontecendo tanto na doutrina francesa, com a dicotomia *contrats informatiques* e *contrats télématiques*, quanto na doutrina espanhola, com a distinção entre *contratación informática* e *contratación por medios informáticos*.”

3 Indicando uma nova era “pós-territorial”, ver, por todos, GOLDSMITH, Jack; WU, Tim. *Who controls the Internet? Illusions of a borderless world*. Oxford: Oxford University Press, 2006, p. 13.

gênese, para a estruturação teórica em torno da declaração de vontade na Rede.⁴

Alertando para a preponderância da forma de se contratar no momento em que há manifestação de vontade, a doutrina fixou a expressão “contrato eletrônico” para se reportar ao “negócio jurídico contratual realizado pela manifestação de vontade, das posições jurídicas ativa e passiva, expressada por meio (...) eletrônico no momento de sua formação”.⁵

O fator preponderante para sua caracterização, portanto, é o meio pelo qual as partes manifestam a vontade. Nesse sentido, há que se registrar a hodierna e importante mudança de comportamento, com redução expressiva do uso de papel – em consolidação ao modelo de sociedade *paperless*⁶ – e migração de diversos negócios jurídicos para o ambiente virtual. Nos dizeres de Fabiano Menke, “agora se vive a realidade de (...) ter de diminuir bastante a necessidade de utilização das assinaturas manuscritas. E isto deve justamente ao desenvolvimento da criptografia assimétrica, e, com ela, a criação das assinaturas digitais.”⁷

4 LORENZETTI, Ricardo Luis. *Tratado de los contratos*. Santa Fe: Rubinzal-Culzoni, 2000, t. 3, p. 850-851, tradução livre. No original: “La mencionada interpretación es problemática, puesto que el “consentimiento electrónico” sería entre presentes porque las declaraciones son instantáneas, y entre ausentes para las reglas del Derecho Internacional Privado, lo cual es frecuente en Internet, ya que los contratos se celebran entre sujetos situados en lugares muy distantes, y en países diferentes. La problematicidad se genera porque se trata de definir conceptualmente lo que es “declaración”, “presencia física”, cuando en realidad, se trata de un problema de atribución del riesgo de las comunicaciones, como lo veremos seguidamente. La cuestión central es, entonces, determinar con precisión el momento de perfeccionamiento del contrato y la legislación aplicable, mediante una regla coherente.”

5 REBOUÇAS, Rodrigo Fernandes. *Contratos eletrônicos: formação e validade*. 2. ed. São Paulo: Almedina, 2018, p. 33.

6 O conceito foi originalmente apresentado por LANCASTER, Frederick. *Toward paperless information systems*. Nova York: Academic Press, 1978.

7 MENKE, Fabiano. *Assinatura eletrônica no direito brasileiro*. São Paulo: Revista dos Tribunais, 2005, p. 30. O autor ainda explica: “As assinaturas eletrônicas, e a espécie assinatura digital, surgem justamente como auxiliar na tarefa de sanar uma imperfeição ínsita das comunicações veiculadas no meio digital, qual seja a de não se ter certeza da identidade da pessoa com a qual se está falando. Enquanto que, no mundo físico, no mais das vezes, se trava contato presencial com a pessoa com quem

Não se inserem nesse conceito, portanto, os instrumentos meramente digitalizados – que, no Brasil, são regidos pela Lei nº 12.682/2012 (Lei da Digitalização) –, mas apenas os documentos: (i) nato-digitais, ou seja, que tenham sido concebidos e estruturados a partir de computadores (com ou sem a utilização da Rede Mundial de Computadores); (ii) os documentos físicos digitalizados e assinados eletronicamente, em conformidade com os mecanismos tecnológicos criados, no país, pela Medida Provisória nº 2.200-2/2001, com observância aos termos da recente reforma implementada pela Lei nº 14.063/2020, em especial em seu art. 4º.

Nada disso se confunde, entretanto, com os contratos inteligentes (*smart contracts*)⁸, originalmente concebidos por Nick Szabo, em 1996⁹, mas que tiveram sua conceituação expandida desde que se concebeu o algoritmo inicial da rede *blockchain*, em outubro de 2008, pelo qual um pseudônimo, Satoshi Nakamoto – não se sabe se adotado por um único indivíduo ou se por um grupo –, detalhou a estrutura de *non-distributed ledgers*¹⁰ que viabilizaria a criação de um mercado para criptoativos (sendo o *Bitcoin* o primeiro deles).¹¹

A evolução do tema, a partir de 2008, foi acentuada, especialmente com o desenvolvimento da plataforma Ethereum, pela qual se tornou

se contratará ou se entabulará algum tipo de comunicação, no mundo virtual essa já não é a regra.”

8 MARTINS, Guilherme Magalhães; FALEIROS JÚNIOR, José Luiz de Moura. Contratos inteligentes (‘smart contracts’) e relações de consumo: equilibrando avanços tecnológicos para proteger os direitos do consumidor. *Revista de Direito do Consumidor*, São Paulo, v. 150, p. 73-108, 2023.

9 SZABO, Nick. *The idea of smart contracts*. Nick Szabo’s Papers and Concise Tutorials, 1997. Disponível em: <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/index.html>. Acesso em: 10 nov. 2025.

10 BASHIR, Imran. *Mastering blockchain: distributed ledger technology, decentralization, and smart contracts explained*. Birmingham: Packt, 2018, p. 12. O autor explica: “Distributed systems are a computing paradigm whereby two or more nodes work with each other in a coordinated fashion to achieve a common outcome. It is modeled in such a way that end users see it as a single logical platform. (...)”

11 ZETZSCHE, Dirk A.; BUCKLEY, Ross P.; ARNER, Douglas W. The distributed liability of distributed ledgers: legal risk of blockchain. *University of New South Wales Law Research Series*, Sydney, v. 17, n. 52, p. 1-49, ago. 2017, p. 2-4.

possível a implementação de *accounts*, em *blockchain* pública, com conteúdo parametrizado e autoexecutado por algoritmos¹² que, supostamente, seriam/são “inteligentes” (a indicar, aliás, inadequada tradução do adjetivo inglês ‘*smart*’).¹³ Essa execução automatizada é geralmente realizada por meio de um computador executando um código que traduz a linguagem jurídica em um programa executável.¹⁴ Este programa tem controle sobre os objetos físicos ou digitais necessários para efetuar a execução. Exemplos: um carro com um programa instalado para impedir a ignição, se os termos de um contrato oneroso inadimplido não forem cumpridos, ou um software bancário que transfira dinheiro automaticamente, se determinadas condições forem atendidas.

Embora a literatura popularize a noção de inteligência, cumpre assinalar que tais scripts não possuem autonomia criativa; limitam-se a executar comandos “*if/then*” codificados *ex ante*. Assim, situam-se numa zona intermediária entre contratos eletrônicos flexíveis e contratações algorítmicas estritas, pois dependem da *blockchain* para *enforcement*, mas carecem de aprendizagem adaptativa em tempo real.¹⁵ Por sua vez, contratos algorítmicos *onchain*, tal como definidos nesta pesquisa, compreendem estruturas autoexecutáveis gravadas diretamente no *ledger*, acrescidas de módulos de inteligência artificial capazes de ajustar parâmetros internos conforme sinais externos, sem alterar o endereço do *bytecode*. Essa camada analítica dota o contrato de certa adaptabilidade estatística, mas não outorga faculdade de

12 DOMINGOS, Richard Henrique; FALEIROS JÚNIOR, José Luiz de Moura; CORDEIRO, Luiz Felipe de Freitas. A legalidade dos ‘smart contracts’ à luz dos requisitos de validade da teoria do negócio jurídico. In: *VII Encontro Virtual do Conpedi*, 2024, Florianópolis - SC. SALEME, Edson Ricardo; LANNES, Yuri Nathan da Costa; SANTOS FILHO, Ronaldo Fenelon (Org.). Direito, governança e novas tecnologias [recurso eletrônico]. Florianópolis: Conpedi, 2024. v. 39. p. 135-156.

13 Sobre o tema, conferir SAVELYEV, Alexander. Contract law 2.0: “smart” contracts as the beginning of the end of classic contract law. *Information & Communications Technology Law*, Londres, v. 26, n. 2, p. 116-134, jan./abr. 2017.

14 RASKIN, Max. The law and legality of smart contracts. *Georgetown Law Technology Review*, Washington, D.C., v. 304, n. 1, p. 305-341, 2017, p. 309-310.

15 FALEIROS JÚNIOR, José Luiz de Moura. *Contratos algorítmicos: conceito, função e interpretação*. Indaiatuba: Foco, 2025, p. 24-25.

ponderação axiológica; logo, se eventos extraordinários escapam às variáveis monitoradas, o script persevera imperturbável, podendo instaurar cenário de onerosidade desarrazoada. Aqui, a imutabilidade do bloco encontra os limites da equidade, evidenciando a necessidade de *circuit breakers* normativamente previstos para suspender execução e permitir renegociação.¹⁶

Um contrato inteligente não depende do acionamento do Estado para que se tenha o *enforcement*, pois as próprias partes contratantes garantiriam o rigoroso desempenho obrigacional a partir da formalização do instrumento.¹⁷ Não há meio termo ou flexibilidade, o que revitaliza o *pacta sunt servanda* como espécie de anátema.

Mas o problema conceitual dos contratos inteligentes não é, em si, técnico. Trata-se de modelo idealizado para um momento no qual seja possível, pela “matematização” da linguagem contratual, delegar todos os elementos conformadores da estrutura clausular das obrigações a um algoritmo “inteligente”, que compreenda, por exemplo, a linguagem natural (falada ou escrita por humanos) e consiga convertê-la em parâmetros matemáticos.

Não se atingiu esse patamar do desenvolvimento tecnológico, ainda, e a própria adjetivação que qualifica tais instrumentos (“inteligentes”) desfalece diante da realidade, embora não se desconsidere a pertinência de seu debate, ainda que a nível especulativo¹⁸.

Surge, porém, campo fértil para um meio-termo, uma proposta mais avançada do que a já consagrada classificação dos contratos

16 FALEIROS JÚNIOR, José Luiz de Moura. *Contratos algorítmicos: conceito, função e interpretação*. Indaiatuba: Foco, 2025, p. 154.

17 O'SHIELDS, Reggie. Smart contracts: legal agreements for the blockchain. *North Carolina Banking Institute Review*, Chapel Hill, v. 21, p. 177-194, 2017, p. 193. Anota: “Blockchain technology and smart contracts have the potential to transform financial markets and the business of banking. At this point, however, this technology is still developing and has not been widely tested in a regulated environment, which leaves open the possibility of unknown operational flaws and vulnerabilities.”

18 FALEIROS JÚNIOR, José Luiz de Moura. Contratos algorítmicos e onerosidade excessiva: as consequências da inflexibilidade. *Civilistica.com - Revista Eletrônica de Direito Civil*, Rio de Janeiro, v. 11, p. 1-13, 2022, p. 9.

eletrônicos, mas de caráter mais concreto e condizente com o atual estágio de desenvolvimento tecnológico.¹⁹

Foi a partir disso que sonoras críticas passaram a nortear a doutrina especializada, que identificava uma incoerência na ideia de autoexecutoriedade obrigacional de contratos que, embora nomeados de inteligentes, ainda são dependentes da capacidade humana de traduzir a linguagem humana (e, inclusive, o jargão jurídico) para linguagem computacional. Uma veleidade, que também é corroborada pelas enfáticas críticas ventiladas por Sklaroff em razão dos “custos da inflexibilidade”.²⁰

Essa problemática já vem sendo enfrentada pela doutrina. Tim Wu tratou do assunto já em 2003²¹, ao passo que Primavera de Filippi e Aaron Wright, por exemplo, alertam mais recentemente para os riscos desse controle exercido pelo código, fazendo trocadilho com a expressão ‘*rule of law*’ (que denominam ‘*rule of code*’), tão utilizada nos sistemas de tradição anglo-saxã²². Por sua vez, a doutrina aponta para a necessidade de que se prime pela natureza não tangencial das estruturas criadas por códigos com aquelas definidas pelas leis.²³⁻²⁴

A solução de equilíbrio adveio de uma formulação conceitual apresentada por Lauren H. Scholz, em 2017²⁵, e que vem sendo estudada com maior atenção em 2021²⁶, inclusive no Brasil, por

19 FALEIROS JÚNIOR, José Luiz de Moura. *Contratos algorítmicos: conceito, função e interpretação*. Indaiatuba: Foco, 2025, p. 39-40.

20 SKLAROFF, Jeremy M. Smart contracts and the cost of inflexibility. *University of Pennsylvania Law Review*, Filadélfia, v. 166, p. 263-303, 2017, p. 302-303.

21 Cf. WU, Tim. When code isn't law. *Virginia Law Review*, Charlottesville v. 89, n. 4, p. 679-412, 2003.

22 DE FILIPPI, Primavera; WRIGHT, Aaron. *Blockchain and the law: the rule of code*. Cambridge: Harvard University Press, 2018, p. 74 *et seq.*

23 TUR FAÚNDEZ, Carlos. *Smart contracts: análisis jurídico*. Madri: Reus, 2018, p. 51-71.

24 TAPSCOTT, Don; TAPSCOTT, Alex. *Blockchain revolution*. Nova York: Penguin, 2016, p. 101-103.

25 Cf. SCHOLZ, Lauren H. Algorithmic contracts. *Stanford Technology Law Review*, Stanford, v. 20, n. 2, p. 128-168, set./dez. 2017.

26 A própria autora explica, em capítulo recentemente publicado: “In a recent article, I coined the term “algorithmic contract” to describe contracts in which an

autores como Orlando Celso da Silva Neto.²⁷ A autora se valeu da expressão “*algorithmic contracts*” (contratos algorítmicos) para descrever um modelo que não é meramente caracterizado pela ‘forma’ e pelo ‘momento’ da manifestação da vontade, mas que também não é totalmente autônomo e ‘inteligente’. Ao descrever tais instrumentos, a expressão *self-driving contracts* (traduzida para o português, por Silva Neto, como ‘contratos algorítmicos autodefinidos’) explicita característica similar à autoexecutoriedade dos contratos inteligentes, mas de escopo de incidência mais restrito.

O ponto distintivo dessa classificação, considerada intermediária, quanto ao conceito já consagrado dos contratos inteligentes é justamente a constatação de que *solvens* e *accipiens* sejam supervisores dos algoritmos implementados para reger as opções definidas no momento da parametrização dos percursos contratuais – matemáticos e autodefinidos – que serão implementados no futuro.²⁸

Surge a dúvida: nesse contexto, como conciliar essa parametrização precoce com eventos supervenientes?

A principal diferença de *design* entre contratos eletrônicos e suas contrapartes algorítmicas reside no *locus* de controle: enquanto o primeiro se ancora em plataformas centralizadas, sujeitas a alterações unilaterais ou bilaterais, o segundo deposita o *enforcement* no consenso criptográfico, blindando-o contra edições subsequentes. Tal transposição de confiança, do ser humano para o parâmetro técnico, repercute diretamente na aplicabilidade do art. 317 do Código Civil, que autoriza o juiz a reajustar prestações diante de motivos imprevisíveis;

algorithm determines the rights and responsibilities of a party by acting as either a gap-filler or a negotiator for the company in the process of contract formation. In gap-filler algorithmic contracts, parties agree that an algorithm, which operates at some time either before or after the contract is formed, will serve as a gap-filler, determining some term in the contract.” SCHOLZ, Lauren H. Algorithms and contract law. In: BARFIELD, Woodrow (Ed.). *The Cambridge Handbook of the Law of Algorithms*. Cambridge: Cambridge University Press, 2021, p. 148.

27 Cf. SILVA NETO, Orlando Celso da. Contratos algorítmicos autodefinidos: introdução e alguns desafios. *Revista de Direito e as Novas Tecnologias*, São Paulo, n.9, out./dez. 2020.

28 FALEIROS JÚNIOR, José Luiz de Moura. *Contratos algorítmicos: conceito, função e interpretação*. Indaiatuba: Foco, 2025, p. 79.

sem cláusula de pausa, a decisão judicial chega tarde, pois o valor já transacionou e permanece registrado no *ledger* de forma irreversível.

Na prática, a porosidade dos contratos algorítmicos aos fatos do mundo depende da qualidade dos oráculos incorporados. Esses serviços, responsáveis por introduzir dados externos na blockchain, podem falhar, atrasarse ou ser corrompidos, produzindo leituras errôneas que potencializam desequilíbrios.²⁹ Diferentemente do contrato eletrônico, em que as partes podem contestar imediatamente a informação recebida, o oráculo defeituoso propagase em cascata, autoexecutando disposições adversas sem janela para contestação. Assim, a robustez do oráculo converte-se em requisito *sine qua non* para reduzir a incidência de onerosidade excessiva em ambientes *onchain* e proteger a equivalência das prestações.

No âmbito da formação, contratos eletrônicos permitem elevado grau de personalização dinâmica, pois cláusulas podem ser editadas até o momento final de aceite. Em contraste, contratos algorítmicos exigem codificação exaustiva das contingências antes da implantação, o que acarreta obstáculo epistemológico: quanto mais complexo o ambiente econômico, maior a chance de fatos supervenientes escaparem ao *script*. Essa limitação de previsibilidade reforça a importância da teoria da base do negócio, lembrando que pactos perduram *rebus sic stantibus*, *i.e.*, enquanto os pressupostos essenciais permanecem intactos, devendo cessar ou ajustar-se quando uma mutação radical lhes subverte o equilíbrio econômico ou jurídico.

Em termos práticos, modificar um contrato eletrônico implica edição de cláusula ou aditivo, com registro em meios tradicionais; já em ecossistemas *onchain*, alterar o código demanda migração para novo endereço, voto de governança ou *hard fork*, operações custosas e, muitas vezes, inviáveis diante da premência do dano. A assimetria procedimental revela que, quanto maior a automação, mais onerosa se torna a correção, invertendo a lógica de eficiência proclamada pelos entusiastas. Nessa senda, a disciplina da onerosidade excessiva

²⁹ BASHIR, Imran. *Mastering blockchain: distributed ledger technology, decentralization, and smart contracts explained*. Birmingham: Packt, 2018, p. 12.

surge como instrumento de compressão dos custos de adaptação, devolvendo plasticidade à avença algoritmizada nos limites de legitimidade contratual vigente.³⁰

Acrescente-se, inicialmente, que toda relação obrigacional é marcada por lacunas e incompletude. A limitação cognitiva das partes, somada à imprevisibilidade estrutural dos mercados, impede a descrição exaustiva de todos os futuros estados do mundo, razão pela qual qualquer pacto contém zonas de silêncio que somente podem ser preenchidas pela hermenêutica judicial ou pela renegociação cooperativa. Nos contratos algorítmicos *on-chain*, essa incompletude adquire contornos tecnológicos: uma vez que o código se autoexecuta a partir de oráculos que injetam dados externos, basta que o feed seja impreciso ou que o evento superveniente extrapole o escopo parametrizado para que surja verdadeira “lacuna digital”, inatingível pelo *script* e por conseguinte refratária ao equilíbrio econômico buscado pelo direito civil.³¹

A presença de lacunas, portanto, reforça a limitação epistemológica dos oráculos. Mesmo sistemas de machine learning sofisticados permanecem circunscritos ao domínio dos dados previamente modelados; logo, eventos extraordinários (*black swans*) continuarão a escapar tanto da previsão estatística quanto da interpretação algorítmica. Essa fragilidade confirma que a justiça contratual não pode ser delegada integralmente ao código — impõe-se preservar mecanismos de intervenção humana (*circuit breakers*, *human approval nodes*) que reintroduzam prudência e sensibilidade valorativa quando o algoritmo silencia diante do inesperado.

Nessa perspectiva, ganha relevo o art. 421-A do Código Civil, inserido pela Lei 13.874/2019 (Lei da Liberdade Econômica).

30 FALEIROS JÚNIOR, José Luiz de Moura. *Contratos algorítmicos: conceito, função e interpretação*. Indaiatuba: Foco, 2025, p. 215-221.

31 DOMINGOS, Richard Henrique; FALEIROS JÚNIOR, José Luiz de Moura; CORDEIRO, Luiz Felipe de Freitas. A legalidade dos ‘smart contracts’ à luz dos requisitos de validade da teoria do negócio jurídico. In: *VII Encontro Virtual do Conpedi*, 2024, Florianópolis - SC. SALEME, Edson Ricardo; LANNES, Yuri Nathan da Costa; SANTOS FILHO, Ronaldo Fenelon (Org.). *Direito, governança e novas tecnologias [recurso eletrônico]*. Florianópolis: Conpedi, 2024. v. 39. p. 135-156.

O dispositivo consagra a autonomia privada para “estabelecer parâmetros objetivos de interpretação das cláusulas, de alocação de riscos e de revisão do contrato”, desde que respeitados a boa-fé, a função social e a vedação ao comportamento contraditório.³² A norma dialoga diretamente com a engenharia contratual algorítmica: permite que as partes, já na etapa de codificação, definam métricas quantitativas (*thresholds* de volatilidade, bandas de preço, índices de inflação) que funcionarão como verdadeiros gatilhos objetivos para ajustes automáticos ou suspensão da execução.

Todavia, a própria estrutura binária do *bytecode* revela que esses parâmetros, por mais detalhados, continuam sujeitos ao dilema da incompletude: ou se produzem regras tão genéricas que perdem utilidade prática, ou se detalham tanto que permanecem vulneráveis a combinações imprevistas de fatos. Em ambos os casos, a reserva de controle judicial subsiste, pois o § 1.º do art. 421-A exige que a interpretação objetiva não afaste “a revisão caso a prestação se torne excessivamente onerosa” — remissão implícita aos arts. 478-480. Desse modo, a superveniência de choque extraordinário fora da curva estatística reabre a porta para o exercício do poder jurisdicional de recompor o sinalagma.³³

3 ONEROSIDADE EXCESSIVA E AS CONSEQUÊNCIAS DA INFLEXIBILIDADE EM ESTRUTURAS AUTOEXECUTÁVEIS ON-CHAIN

Discussões sobre o regime geral da “onerosidade excessiva”, no Brasil, compreendem o escopo de incidência dos artigos 478, 479 e 480 do Código Civil. O primeiro dispositivo tem requisitos explícitos: exige-se contrato de execução continuada ou diferida, a excessiva

32 FALEIROS JÚNIOR, José Luiz de Moura. *Contratos algorítmicos: conceito, função e interpretação*. Indaiatuba: Foco, 2025. No prelo.

33 FALEIROS JÚNIOR, José Luiz de Moura. Contratos algorítmicos e onerosidade excessiva: as consequências da inflexibilidade. *Civillistica.com - Revista Eletrônica de Direito Civil*, Rio de Janeiro, v. 11, p. 1-13, 2022, p. 10.

onerosidade da prestação para uma das partes; a presença de elemento causal imprevisível e extraordinário, que não gera o desaparecimento da finalidade pretendida pelas partes, mas acarreta dificuldade extraordinária para o cumprimento da prestação.

É justamente nesse ponto que emergem os chamados *circuit breakers*, concebidos como mecanismos de suspensão emergencial da autoexecutoriedade. Esses dispositivos, quando corretamente parametrizados, permitem que a lógica determinística do contrato seja temporariamente interrompida, impedindo que a execução continue avançando em cenários de intensa volatilidade ou de choques extraordinários. Embora não substituam a tutela jurisdicional, tais mecanismos introduzem, na esfera algorítmica, uma válvula de contenção que aproxima a execução automatizada dos valores corretivos da teoria da onerosidade excessiva.

A leitura do dispositivo já revela a incompatibilidade do instituto com a discussão sobre os contratos inteligentes, pois “como a execução se dá automática e autonomamente, inexistente, a priori, a possibilidade de interrompê-la, arcando as partes com os ônus do evento não previsto.”³⁴ O fenômeno da onerosidade excessiva, embora antigo, revela nova feição diante da inalterabilidade dos contratos algorítmicos *onchain*: a execução cega converte-se em verdadeira “fatalidade codificada”, pois o *bytecode* não distingue entre perturbações ordinárias e cataclísmicas. A dogmática civilista, todavia, não abdica do imperativo de justiça; o juiz, ainda que a transação esteja registrada em bloco imutável, pode reconhecer o desequilíbrio superveniente e condenar ao ressarcimento equivalente, restaurando a equivalência patrimonial. Assim, a inflexibilidade técnica não exime o direito de corrigir o sacrifício exacerbado.

Nos contratos bilaterais, a consequência, se presentes essas condicionantes, a solução é a resolução do contrato. Excepcionalmente, prevê o dispositivo seguinte (art. 479) a possibilidade de modificação

34 DIVINO, Sthéfano Bruno Santos. Smart contracts: conceitos, limitações, aplicabilidade e desafios. *Revista Jurídica Luso-Brasileira*, Lisboa, ano 4, n. 6, p. 2771-2808, 2018, p. 2801.

equitativa, desde que oferecida pela parte contrária. Já nos contratos unilaterais, prevê o terceiro dispositivo (art. 480) a redução da prestação ou a alteração de seu ‘modo de execução’ (leia-se: revisão), embora não fique claro se, para os contratos unilaterais, devem estar presentes os requisitos adicionais do artigo 478 do Código.

O tema desperta curiosidade porque parece que se está priorizando a conservação do negócio jurídico, pela revisão, como efetiva opção preferencial à resolução.³⁵ Isso causa estranheza, naturalmente, pois facultar ao devedor a postulação judicial da revisão do contrato por onerosidade excessiva – e não apenas sua resolução, como consta do art. 478 – significaria impor ao credor a aceitação de condições contratuais que, possivelmente, não teria aceitado por ocasião da contratação, impondo-lhe ônus não consentido e superveniente.³⁶

Tudo isso revela certa permeabilidade ao princípio *pacta sunt servanda*³⁷ e, no âmbito das diversas classificações contratuais, já indica uma primeira limitação, pois se torna nebulosa a viabilidade de incidência da previsão aos tipos aleatórios, eis que, por sua própria natureza ou por terem as próprias partes condicionado o vínculo a tal condicionante, estariam os contratantes assumindo conscientemente

35 O referido entendimento, aliás, foi consolidado no enunciado nº 176, das III Jornadas de Direito Civil do Conselho da Justiça Federal: “Em atenção ao princípio da conservação dos negócios jurídicos, o art. 478 do Código Civil de 2002 deverá conduzir, sempre que possível, à revisão judicial dos contratos e não à resolução contratual.”

36 MARINO, Francisco Paulo de Crescenzo. *Revisão contratual*: onerosidade excessiva e modificação contratual equitativa. São Paulo: Almedina, 2020, p. 73.

37 O tema ganhou contornos acentuados, no Brasil, a partir de influência do modelo italiano, cujo artigo 1.467, alínea 1, do Código Civil de 1942 – um dos primeiros da Europa, no século XX – teve grande impacto na construção do projeto de renovação do Código Civil brasileiro, elaborado em 1972. Sobre o tema, conferir, por todos, RODRIGUES JÚNIOR, Otavio Luiz. *Revisão judicial dos contratos*: autonomia da vontade e teoria da imprevisão. São Paulo: Atlas, 2016, p. 157-158. Ainda sobre o tema, anota Fábio Siebeneichler de Andrade que “constitui esta opção uma aproximação entre o Direito brasileiro e o Direito italiano, a partir da codificação de 2002, na medida em que desconsiderou as referências à teoria da base do negócio e à teoria da imprevisão, respectivamente de origem germânica e francesa.” ANDRADE, Fábio Siebeneichler de. A teoria da onerosidade excessiva no direito civil brasileiro: limites e possibilidades de sua aplicação. *Revista da Ajuris*, Porto Alegre, v. 41, n. 134, p. 236-261, jun. 2014, p. 242.

as consequências de que a prestação se torne excessivamente onerosa para um ou outro.

Outra questão a se considerar diz respeito à não incidência de tais dispositivos a contratos de consumo – regidos por legislação própria –, que constituem a grande gama de modelos indicados pela doutrina como contratos eletrônicos.³⁸

A presente investigação concerne às relações civis e empresariais, portanto, e o artigo 478, além de exigir que a prestação se torne excessivamente onerosa, pressupõe a configuração de extrema vantagem para o credor, situação subjetiva e de difícil aferição em modelos estritamente matemáticos pelo simples fato de fórmulas e equações não serem capazes de revelar as circunstâncias e particularidades da vida em toda a sua complexidade.

Nos dizeres de Karen Levy, “*smart contracts are not so smart*”, uma vez que a complexidade das relações humanas pode apresentar desafios – especialmente no momento do *enforcement* – que apenas a ponderação e a razoabilidade poderiam conceber. A autora, aliás, aponta três comportamentos capazes de enviesar as relações contratuais no atual estado da técnica: a) redigir ou ceder a termos que não se pretenda executar (*writing or acceding to unenforceable terms*): nesta situação, são definidas expectativas quanto a comportamentos futuros, inclusive fora do âmbito estrito do contrato, como desdobramentos que, no Brasil, se poderia colher da boa-fé objetiva; b) redigir ou ceder a termos muito vagos (*writing or acceding to purposefully vague terms*): esta prática cria uma camada mais flexível para alinhamentos posteriores, especialmente nas relações de trato sucessivo e nos contratos relacionais; c) opção deliberada pela não execução de termos que são executáveis (*willful nonenforcement of enforceable terms*): além da mera liberalidade que indica, permite um recurso estratégico de negociação para que se opere fora do Judiciário.³⁹

38 MARTINS, Guilherme Magalhães. *Contratos eletrônicos de consumo*. 3. ed. São Paulo: Atlas, 2016, p. 42.

39 LEVY, Karen E. C. *Book-smart, not street-smart: blockchain-based smart contracts and the social workings of law. Engaging Science, Technology, and Society*, Boston, v. 3, p. 1-15, 2017, p. 5-6.

Esse gatilho suspensivo é justamente um dos papéis potenciais dos *circuit breakers*, que podem ser programados para congelar determinadas funções contratuais sempre que parâmetros de risco ultrapassarem limiares pré-definidos. No entanto, sua eficácia depende da completude dos dados alimentados pelos oráculos, e a incompletude desses *inputs* pode, paradoxalmente, acionar ou deixar de acionar o estado de pausa de forma inadequada.

A onerosidade excessiva, recorde-se, não prescinde de três requisitos clássicos: imprevisibilidade, extraordinariedade e excessiva onerosidade. Nas estruturas *onchain*, o segundo elemento ganha contornos estatísticos, pois a volatilidade própria do mercado cripto já se encontra presumida. Assim, somente choques acima de desviopadrão histórico é que se qualificam como “extraordinários”. Essa métrica confere objetividade à cláusula, permitindo que o algoritmo identifique automaticamente o ponto de inflexão e acione gatilho suspensivo, sem depender de interpretação humana prévia.⁴⁰

E, sobre isso, ressalte-se que, “caso as partes visualizem que a modificação extrajudicial é economicamente inviável, uma segunda direção é aquela que poderá relevar e utilizar a revisão judicial. Ainda que os custos dessa possam ser menores, seriam incomparáveis com as modificações e alterações extrajudiciais que poderiam ser realizadas em um contrato não inteligente”.⁴¹

Nesse contexto, os *smart contracts* apresentarão uma dimensão adicional quando o controle for exercido à distância pelo fornecedor que detém a ciência do inadimplemento (como nos exemplos de serviços de *streaming* ou de armazenamento em nuvem, que não se valem necessariamente da *blockchain*, mas fazem cessar a prestação de serviço, de forma sumária e automatizada, em caso de inadimplemento). Para Jonathan Zittrain, essas operações de controle e ativação de gatilhos à distância (*tethered operations*) seriam

40 BASHIR, Imran. *Mastering blockchain: distributed ledger technology, decentralization, and smart contracts explained*. Birmingham: Packt, 2018, p. 15.

41 DIVINO, Sthéfano Bruno Santos. Smart contracts: conceitos, limitações, aplicabilidade e desafios. *Revista Jurídica Luso-Brasileira*, Lisboa, ano 4, n. 6, p. 2771-2808, 2018, p. 2801.

como maçanetas, ativáveis a partir do implemento de condições pré-concebidas que dependem de dados e que são acionadas fora do dispositivo que o usuário utiliza para se valer do cumprimento da prestação.⁴²

O risco que se corre, entretanto, concerne à indesejável autotutela que isto gera para operações variadas, empoderando uma das partes – a que terá condições de determinar o acionamento do gatilho – embora o resultado não difira do tradicional inadimplemento, haja vista a correlata inação do contratante.

Com arrimo na economia e na análise dos custos de transação⁴³, pode-se constatar que, “em certas situações, a melhor opção disponível para o devedor poderá ser descumprir o contrato. Isso ocorrerá sempre que os custos com o cumprimento superarem os custos com as consequências do inadimplemento”.⁴⁴ Nada disso é possível em contratos algorítmicos autodefinidos, pois inexistente a opção de inadimplir. Nos dizeres de Lauren H. Scholz: “Esta abordagem, para avaliar contratos algorítmicos, apresenta resultados melhores ao atingir as metas de redução de externalidades e preservação do jogo justo no comércio do que no *status quo* ambíguo de ignorar contratos algorítmicos como uma categoria especial de acordos. A abordagem faz isso ao mesmo tempo em que faz jus às ações e riscos assumidos pelas partes do acordo. Dito de outra forma, esta abordagem multifacetada para contratos algorítmicos permite que a lei mantenha acordos algorítmicos quando eles são feitos de forma justa, mas produz reequilíbrio justamente quando eles não são”.⁴⁵

42 ZITTRAIN, Jonathan. Perfect enforcement on tomorrow's Internet. In: BROWNSWORD, Roger; YEUNG, Karen (Es.). *Regulating technologies: legal futures, regulatory frames and technological fixes*. Oxford: Hart Publishing, 2008, p. 131.

43 WILLIAMSON, Oliver E. Transaction-cost economics: The governance of contractual relations. *Journal of Law and Economics*, Chicago, v. 22, n. 2, p. 233-261, out. 1979, p. 261. Anota: “Transaction-cost economics is an interdisciplinary undertaking that joins economics with aspects of organization theory and overlaps extensively with contract law.”

44 LOPES, Christian Sahb Batista. *Mitigação dos prejuízos no direito contratual*. São Paulo: Saraiva, 2013, p. 101.

45 SCHOLZ, Lauren H. Algorithmic contracts. *Stanford Technology Law Review*, Stanford, v. 20, n. 2, p. 128-168, set./dez. 2017, p. 167, tradução livre. No original: “This

No contexto analisado pela autora no trecho transcrito, é imaginado um cenário em que mecanismos de controle sejam implementados pelas partes para que haja o desejável distanciamento do modelo dos contratos inteligentes, em que não há saídas.⁴⁶ A autora exemplifica citando que um gestor poderia, por exemplo se valer de um algoritmo de detecção (*stalking algorithm*) para fiscalizar, em tempo real, ações relevantes adotadas pelo algoritmo de regência contratual; ainda, como alternativa, Scholz faz menção aos seguros contra riscos de falhas decorrentes da incerteza algorítmica – embora o faça de forma vaga e não convincente, haja vista a inerente dificuldade de se conceber a securitização daquilo que se desconhece – e, por fim, a autora sugere a introdução de *human approval nodes*, semelhantes aos gatilhos de validação remota nas *tethered operations*, sugeridos por Zittrain.

Em complemento, os *circuit breakers* ocupam posição intermediária entre a rigidez absoluta dos *smart contracts* e a flexibilidade dos contratos tradicionais, introduzindo uma “janela de contenção” que, ao menos teoricamente, pode impedir que a autoexecutoriedade agrave ainda mais o desequilíbrio superveniente – embora sem garantir, por si só, a recomposição integral do sinalagma.

Mesmo assim, ainda há várias questões em aberto e que desafiam a cogitação de instituto complexo como o da onerosidade excessiva para modelos contratuais algorítmicos autodefinidos. Ainda que se considere a utilização de gatilhos ou nós de validação, indagações sobre a tecnologia por trás desses instrumentos revelam o ambiente recôndito de sua implementação; ademais, questões de responsabilidade civil quanto aos erros de programação dos

approach to evaluating algorithmic contracts does a better job at achieving the goals of reducing externalities and preserving fair play in commerce than the ambiguous status quo of ignoring algorithmic contracts as a special category of agreement. The approach does this while doing justice to the actions and risks assumed by the parties to the agreement. Put another way, this multi-pronged approach to algorithmic contracts allows the law to uphold algorithmic agreements when they are fairly made, but rightfully gives relief when they are not.”

46 SKLAROFF, Jeremy M. Smart contracts and the cost of inflexibility. *University of Pennsylvania Law Review*, Filadélfia, v. 166, p. 263-303, 2017, p. 303.

parâmetros estabelecidos geram inquietações; finalmente, dúvidas sobre como tratar os efeitos deletérios das falhas humanas quanto à definição dos objetivos do pacto e das instruções de programação também revelam a incipiência do debate.

Não há dúvidas de que a garantia de segurança e equilíbrio negocial é incompatível, com tais modelos, ao menos atualmente. Eventual revisão futura, que acompanhará o próprio desenvolvimento tecnológico, poderá revelar o oposto, mas a aplicação desses instrumentos – que já são tecnologicamente viáveis – deve se restringir a pactos civis ou empresariais de cunho mais trivial e previsível, afastando-se qualquer perspectiva ou expectativa de revisão dos termos pactuados por onerosidade excessiva.

A inserção de limites percentuais de variação incidente sobre a prestação não logra aferir com a devida precisão se o cumprimento contratual assumiu uma onerosidade efetivamente excessiva. Mesmo uma oscilação que ultrapasse determinado limiar pode não caracterizar, sob o prisma jurídico, um desequilíbrio suficientemente grave para justificar a aplicação dos arts. 478 a 480 do Código Civil. Por outro lado, variações inferiores a esse índice, em certos contextos, podem ser suficientes para desestruturar o sinalagma contratual, a depender das condições iniciais e dos riscos assumidos. A ausência de flexibilidade para interpretar e sopesar esses cenários no momento da execução resulta, portanto, em juízos automatizados que não refletem a análise circunstancial exigida pela onerosidade excessiva⁴⁷.

Um exemplo ilustrativo recai sobre um contrato algorítmico de fornecimento de energia elétrica, estruturado na forma de um *Service Level Agreement* (SLA), em que o valor do fornecimento é ajustado de forma automática conforme variações diárias em índices de mercado ou em métricas de demanda⁴⁸. Suponha-se que o contrato algorítmico esteja programado para, a cada intervalo regular, recolher dados de

47 SKLAROFF, Jeremy M. Smart contracts and the cost of inflexibility. *University of Pennsylvania Law Review*, Filadélfia, v. 166, p. 263-303, 2017, p. 280.

48 DUBICKIS, Mikus; GAILE-SARKANE, Elina. Perspectives on Innovation and Technology Transfer. *Procedia - Social and Behavioral Sciences*, [S.l.], v. 213, p. 965-970, 2015, p. 967.

um oráculo acerca do custo de geração, da cotação de combustíveis e de fatores como condições climáticas que impactam a oferta de energia. Em tempos de normalidade, a lógica algorítmica processa essas informações, aplica um percentual de variação e atualiza o preço final a ser pago.

O problema surge se houver um conjunto de eventos excepcionais (por exemplo, interrupção imprevista no abastecimento de insumos energéticos, catástrofe ambiental em região fornecedora e aumento abrupto de impostos) que eleve drasticamente o custo de geração ou transporte de energia para níveis muito além do previsível no momento da pactuação. Em razão da execução inflexível do código, o contrato – ainda que formalmente concebido como SLA – continuaria aplicando reajustes automáticos sem avaliar se o impacto resultante ultrapassou o limite normal de sacrifício empresarial⁴⁹. Se o encarecimento ultrapassar significativamente o que a indústria pode suportar, desconfigurando as bases econômicas do acordo e tornando inviável a continuidade do negócio, poder-se-ia caracterizar a onerosidade excessiva. Todavia, o contrato algorítmico, por não possuir cláusulas de salvaguarda ou mecanismos de renegociação embutidos, persistiria em exigir o pagamento, desencadeando uma situação em que somente a invocação dos arts. 478 a 480 do Código Civil, ou o consentimento voluntário do credor em rever as condições, poderia restabelecer o equilíbrio do sinalagma contratual.

49 Nesse panorama, um contrato algorítmico *offchain*, concebido em Python ou em outra linguagem de programação, seria configurado para consultar periodicamente uma ou mais APIs, com o intuito de reunir dados concernentes aos custos energéticos, à disponibilidade de insumos e às eventuais variações tributárias. As rotinas internas, de forma automatizada, processariam essas informações e recalculariam o valor final em intervalos predefinidos – por exemplo, uma vez ao dia –, aplicando a lógica inscrita no código, desprovida de qualquer análise circunstancial mais aprofundada. Em caso de eventos extraordinários, tais como a interrupção imprevista no fornecimento de matérias-primas ou a majoração abrupta de impostos, o algoritmo, devido à sua natureza rígida, se limitaria a atualizar os registros internos e refletir esses acréscimos no custo a ser arcado pelo comprador, sem aferir se o aumento ultrapassaria o limite normalmente suportável pela parte mais vulnerável. Por conseguinte, a autoexecução do *script* se manteria, impondo o pagamento de valores revisados que, embora manifestamente onerosos, não seriam objeto de qualquer ponderação quanto à previsibilidade inicial do SLA.

O atual estado da técnica não permite aferir com plena acurácia se o encarecimento decorrente de um conjunto de eventos extraordinários efetivamente caracteriza uma onerosidade excessiva. Não obstante se possa introduzir parâmetros quantitativos (como percentuais de variação), a identificação de um desequilíbrio suficientemente grave para cumprir os requisitos dos arts. 478 a 480 do Código Civil demanda uma análise contextual de elementos econômicos e subjetivos que a execução puramente algorítmica ainda não contempla. Por esse motivo, ganha relevo a adoção de gatilhos contratuais, ou seja, mecanismos de interrupção ou suspensão que permitem que o contrato deixe de se executar automaticamente diante de um cenário indicativo de onerosidade anômala, facultando às partes a oportunidade de avaliar a real dimensão do desequilíbrio antes que a execução rígida agrave o problema.

Nos contratos *on-chain* – especialmente os que se desenvolvem em plataformas como Ethereum (EVM) – esses gatilhos costumam ser designados “*circuit breakers*” ou “*emergency stops*”⁵⁰. Trata-se de rotinas em *Solidity* que, mediante a detecção de uma condição excecional (por exemplo, por meio de oráculos que reportam variações abruptas de preço ou outros dados imprevistos), ativam um estado de pausa. Nesse estado, determinadas funções do contrato ficam bloqueadas até que se verifique a viabilidade de retomar a execução sem violar os princípios contratuais subjacentes.

Ainda assim, tais mecanismos são paliativos: mitigam, mas não eliminam, a tensão estrutural entre autoexecutoriedade e justiça contratual, pois sua própria lógica permanece presa à parametrização *ex ante*, sujeita às limitações cognitivas e técnicas que originam a onerosidade excessiva no ambiente algorítmico.

50 ANTONOPOULOS, Andreas M.; WOOD, Gavin. *Mastering Ethereum: bulding smart contracts and DApps*. Sebastopol: O’Reilly, 2019, p. 688.

4 CONCLUSÃO

O desenvolvimento algorítmico é crescente e irrefreável. Novas discussões acerca dos impactos de tecnologias emergentes sobre institutos teóricos tradicionais continuarão a gerar problemas variados e, no que concerne aos contratos, os desafios são inúmeros. Como se viu, de forma sintética, os contratos eletrônicos marcaram uma fase desafiadora para a compreensão dos impactos do uso da tecnologia na expressão da vontade em seu aspecto formal (por meio eletrônico), demandando, ainda, análise quanto ao momento da celebração do negócio jurídico. Noutro extremo, em averiguação prospectiva, têm-se os contratos algorítmicos *on-chain* como modelos tecnicamente imutáveis e estáveis, voltados à autoexecutoriedade dos parâmetros obrigacionais, mas sem qualquer flexibilidade ou permeabilidade para intervenções supervenientes.

Sendo certo que algoritmos já regem atividades desenvolvidas contratualmente e, devido à incompatibilidade das duas categorias citadas com os modelos tecnológicos atuais – que já não são aqueles da década de 1990 e tampouco correspondem aos pujantes modelos efetivamente “inteligentes” –, a doutrina sinaliza a incorporação de um modelo intermediário, o dos contratos algorítmicos autodefinidos, que mantêm a autoexecutoriedade típica dos *smart contracts*, mas impõem aos contratantes os ônus decorrentes de sua adoção. Noutro giro, reitera-se que a inflexibilidade codificada agrava problema de *path dependence*: decisões iniciais de desenho condicionam inexoravelmente futuros percursos algorítmicos. Se, na fase de programação, se negligenciam cláusulas de pausa, o sistema internaliza trajetória de fatalismo, na qual a execução se desenrola independentemente de choques supervenientes que comprometam o equilíbrio do sinalagma.

Nesse contexto, a introdução de *circuit breakers* ou *emergency stops* – rotinas que permitem suspender temporariamente a autoexecutoriedade diante de determinados gatilhos objetivos – apresenta-se como tentativa relevante de aproximar a engenharia

contratual algorítmica das exigências de justiça contratual. Esses mecanismos, aliados a *human approval nodes* e a parâmetros quantitativos pré-definidos, funcionam como válvulas de escape para evitar que eventos extraordinários se convertam em sacrifícios patrimoniais desmesurados. Ainda assim, trata-se de mitigação parcial: a decisão sobre quando acionar o freio de emergência continua dependente de escolhas pré-programadas e da qualidade dos oráculos, de modo que os arts. 478 a 480 do Código Civil permanecem, em grande medida, reféns da arquitetura técnica adotada.

Logo, dispositivos como os arts. 478, 479 e 480 do Código Civil brasileiro revelam-se, no atual estado da técnica, estruturalmente tensionados quando confrontados com contratos algorítmicos autodefinidos estritos, o que realça a pujança do tema-problema. Os *circuit breakers* representam um ponto de contato promissor entre a dogmática da onerosidade excessiva e o desenho de estruturas *on-chain*, mas não afastam a constatação de que a justiça contratual ainda não pode ser integralmente delegada ao código. No futuro, com a evolução tecnológica e a sofisticação dos mecanismos de pausa, supervisão e revisão embarcada, esse debate poderá ser revisitado; por ora, contudo, confirma-se a hipótese de que a revisão por onerosidade excessiva permanece, em larga medida, incompatível com contratos algorítmicos autodefinidos puros, impondo às partes o dever de ponderar, *ex ante*, se o ganho de eficiência oferecido pela autoexecutoriedade compensa o preço de uma flexibilidade drasticamente reduzida.

REFERÊNCIAS

ANDRADE, Fábio Siebeneichler de. A teoria da onerosidade excessiva no direito civil brasileiro: limites e possibilidades de sua aplicação. *Revista da Ajuris*, Porto Alegre, v. 41, n. 134, p. 236-261, jun. 2014.

ANTONPOULOS, Andreas M.; WOOD, Gavin. *Mastering Ethereum: building smart contracts and DApps*. Sebastopol: O'Reilly, 2019.

BASHIR, Imran. *Mastering blockchain: distributed ledger technology, decentralization, and smart contracts explained*. Birmingham: Packt, 2018.

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

DE LUCCA, Newton. *Aspectos jurídicos da contratação informática e telemática*. São Paulo: Saraiva, 2003.

DIVINO, Sthéfano Bruno Santos. Smart contracts: conceitos, limitações, aplicabilidade e desafios. *Revista Jurídica Luso-Brasileira*, Lisboa, ano 4, n. 6, p. 2771-2808, 2018.

DOMINGOS, Richard Henrique; FALEIROS JÚNIOR, José Luiz de Moura; CORDEIRO, Luiz Felipe de Freitas. A legalidade dos 'smart contracts' à luz dos requisitos de validade da teoria do negócio jurídico. In: *VII Encontro Virtual do Conpedi*, 2024, Florianópolis - SC. SALEME, Edson Ricardo; LANNES, Yuri Nathan da Costa; SANTOS FILHO, Ronaldo Fenelon (Org.). *Direito, governança e novas tecnologias [recurso eletrônico]*. Florianópolis: Conpedi, 2024. v. 39. p. 135-156.

DUBICKIS, Mikus; GAILE-SARKANE, Elina. Perspectives on Innovation and Technology Transfer. *Procedia - Social and Behavioral Sciences*, [S.l.], v. 213, p. 965-970, 2015.

FALEIROS JÚNIOR, José Luiz de Moura. *Contratos algorítmicos: conceito, função e interpretação*. Indaiatuba: Foco, 2025.

FALEIROS JÚNIOR, José Luiz de Moura. Contratos algorítmicos e onerosidade excessiva: as consequências da inflexibilidade. *Civilistica.com - Revista Eletrônica de Direito Civil*, Rio de Janeiro, v. 11, p. 1-13, 2022.

GOLDSMITH, Jack; WU, Tim. *Who controls the Internet? Illusions of a borderless world*. Oxford: Oxford University Press, 2006.

LANCASTER, Frederick. *Toward paperless information systems*. Nova York: Academic Press, 1978.

LEVY, Karen E. C. Book-smart, not street-smart: blockchain-based smart contracts and the social workings of law. *Engaging Science, Technology, and Society*, Boston, v. 3, p. 1-15, 2017.

LOPES, Christian Sahb Batista. *Mitigação dos prejuízos no direito contratual*. São Paulo: Saraiva, 2013.

LORENZETTI, Ricardo Luis. *Tratado de los contratos*. Santa Fe: Rubinzal-Culzoni, 2000, t. 3.

MARINO, Francisco Paulo de Crescenzo. *Revisão contratual: onerosidade excessiva e modificação contratual equitativa*. São Paulo: Almedina, 2020.

MARTINS, Guilherme Magalhães. *Contratos eletrônicos de consumo*. 3. ed. São Paulo: Atlas, 2016.

MARTINS, Guilherme Magalhães; FALEIROS JÚNIOR, José Luiz de Moura. Contratos inteligentes ('smart contracts') e relações de consumo: equilibrando avanços tecnológicos para proteger os direitos do consumidor. *Revista de Direito do Consumidor*, São Paulo, v. 150, p. 73-108, 2023.

MENKE, Fabiano. *Assinatura eletrônica no direito brasileiro*. São Paulo: Revista dos Tribunais, 2005.

O'SHIELDS, Reggie. Smart contracts: legal agreements for the blockchain. *North Carolina Banking Institute Review*, Chapel Hill, v. 21, p. 177-194, 2017.

RASKIN, Max. The law and legality of smart contracts. *Georgetown Law Technology Review*, Washington, D.C., v. 304, n. 1, p. 305-341, 2017.

REBOUÇAS, Rodrigo Fernandes. *Contratos eletrônicos: formação e validade*. 2. ed. São Paulo: Almedina, 2018.

RODRIGUES JÚNIOR, Otavio Luiz. *Revisão judicial dos contratos: autonomia da vontade e teoria da imprevisão*. São Paulo: Atlas, 2016.

SAVELYEV, Alexander. Contract law 2.0: “smart” contracts as the beginning of the end of classic contract law. *Information & Communications Technology Law*, Londres, v. 26, n. 2, p. 116-134, jan./abr. 2017.

SILVA NETO, Orlando Celso da. Contratos algorítmicos autodefinidos: introdução e alguns desafios. *Revista de Direito e as Novas Tecnologias*, São Paulo, n.9, out./dez. 2020.

SCHOLZ, Lauren H. Algorithmic contracts. *Stanford Technology Law Review*, Stanford, v. 20, n. 2, p. 128-168, set./dez. 2017.

SCHOLZ, Lauren H. Algorithms and contract law. In: BARFIELD, Woodrow (Ed.). *The Cambridge Handbook of the Law of Algorithms*. Cambridge: Cambridge University Press, 2021.

SKLAROFF, Jeremy M. Smart contracts and the cost of inflexibility. *University of Pennsylvania Law Review*, Filadélfia, v. 166, n. 1, p. 263-303, 2017.

SZABO, Nick. *The idea of smart contracts*. Nick Szabo's Papers and Concise Tutorials, 1997. Disponível em: <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/index.html>. Acesso em: 10 nov. 2025.

TAPSCOTT, Don; TAPSCOTT, Alex. *Blockchain revolution*. Nova York: Penguin, 2016.

TUR FAÚNDEZ, Carlos. *Smart contracts: análisis jurídico*. Madri: Reus, 2018.

WILLIAMSON, Oliver E. Transaction-cost economics: The governance of contractual relations. *Journal of Law and Economics*, Chicago, v. 22, n. 2, p. 233-261, out. 1979.

WU, Tim. When code isn't law. *Virginia Law Review*, Charlottesville v. 89, n. 4, p. 679-412, 2003.

ZETZSCHE, Dirk A.; BUCKLEY, Ross P.; ARNER, Douglas W. The distributed liability of distributed ledgers: legal risk of blockchain. *University of New South Wales Law Research Series*, Sydney, v. 17, n. 52, p. 1-49, ago. 2017.

ZITTRAIN, Jonathan. Perfect enforcement on tomorrow's Internet. In: BROWNSWORD, Roger; YEUNG, Karen (Ed.). *Regulating technologies: legal futures, regulatory frames and technological fixes*. Oxford: Hart Publishing, 2008.

2. SMART CONTRACTS E DIREITOS AUTORAIS

Manuela Machado Gonçalves

Especialista em Direito Digital pelo Instituto de Tecnologia e Sociedade do Rio de Janeiro – ITS Rio, em parceria com o Centro de Estudos e Pesquisas no Ensino do Direito da Universidade do Estado do Rio de Janeiro (CEPED/ UERJ).

INTRODUÇÃO

A economia do entretenimento é impactada por duas forças simultâneas: (i) a digitalização das cadeias de distribuição, com streaming, plataformas on-demand e novos modelos de monetização; e (ii) a crescente complexidade de direitos e fluxos de pagamento, que passam por múltiplos intermediários (produtores, distribuidoras, agregadoras, plataformas, sociedades de gestão coletiva, subeditores e agentes internacionais). Em consequência, discussões que antes se restringiam à negociação privada de contratos hoje se deslocam para o desenho de sistemas de governança de dados e de prestação de contas.

No Brasil, a assimetria informacional aparece de forma particularmente nítida na comparação entre os setores musical e audiovisual. No mercado musical, a Lei nº 9.610/1998 (Lei de Direitos Autorais – LDA) organiza a autorização e a remuneração pela execução pública de obras musicais e fonogramas e prevê a gestão coletiva por associações e pelo ente arrecadador unificado, cujo papel é exercido pelo ECAD (arts. 97 a 100). (BRASIL, 1998).

Já no audiovisual, embora a LDA reconheça direitos de autor e direitos conexos (incluindo os direitos de artistas intérpretes ou executantes, como atores, no art. 90), a remuneração por reexibições e pela exploração em novas mídias tende a ser definida caso a caso, por contrato, e muitas vezes se concentra em pagamentos únicos (cachês e cláusulas de buyout). (BRASIL, 1998).

A pressão contemporânea por ajustes decorre, em grande medida, do deslocamento do consumo para serviços digitais e da migração de catálogos para streaming. No Senado Federal tramita propostas legislativas que buscam instituir remuneração residual para obras audiovisuais executadas na internet, independentemente de contratos, o que evidencia que o tema se tornou uma questão regulatória em debate no país. (SENADO FEDERAL, 2025).

Nesse cenário, tecnologias como blockchain e contratos inteligentes passaram a ser apresentadas como instrumentos para criar trilhas de auditoria confiáveis, registrar eventos de exploração e executar automaticamente regras de distribuição (splits) pactuadas entre titulares.

A promessa mais realista não é substituir o contrato tradicional por código, mas desenhar contratos híbridos (smart legal contracts) que combinem texto jurídico – interpretável e revisável – com automação de cláusulas objetivamente mensuráveis, como cálculo de percentuais e pagamentos. (MIT DCI, 2016; FERRO et al., 2023).

O objetivo deste artigo é (a) descrever o funcionamento do ECAD e seu modelo de arrecadação e distribuição; (b) apresentar a problemática da remuneração no audiovisual, com foco em reexibições e licenciamento; (c) discutir ganhos e riscos; e (d) propor como smart contracts poderiam operar na distribuição automática de royalties, com base em iniciativas existentes e na realidade normativa brasileira.

1. DIREITOS AUTORAIS

A LDA protege direitos morais e patrimoniais de autores e prevê, no Título V, os direitos conexos, aplicando-se – no que couber – aos artistas intérpretes ou executantes, produtores e empresas de radiodifusão (art. 89). Para os intérpretes e executantes, o art. 90 elenca, entre outros, o direito exclusivo de autorizar ou proibir a fixação, reprodução, execução pública, radiodifusão e a colocação à

disposição do público de suas interpretações ou execuções. (BRASIL, 1998).

O reconhecimento legal, entretanto, não resolve automaticamente a pergunta econômica central: como e quando esses direitos geram remuneração na prática cotidiana?

No audiovisual, especialmente em obras encomendadas por grandes players (emissoras, plataformas ou financiadores), é comum que contratos busquem concentrar a remuneração em pagamentos iniciais e ampliar cessões/licenças para múltiplos territórios, mídias e janelas. Esse fenômeno é frequentemente descrito como buyout – a cessão ampla de direitos patrimoniais em troca de pagamento único – e é objeto de preocupação em diretrizes internacionais. Por exemplo, a CISAC (Confederação Internacional das Sociedades de Autores e Compositores) descreve buyout como cláusulas em que autores aceitam abrir mão do controle e da participação em receitas futuras, em troca de quantia única. (CISAC).

A dinâmica de “pagamento único” não significa ausência absoluta de remuneração por reexibições (há casos de pagamentos residuais ou acordos coletivos em segmentos específicos), mas revela uma tendência estrutural: quando não há um sistema coletivo robusto e padronizado para capturar eventos de exploração e distribuir receitas, a remuneração tende a depender do poder de barganha contratual, e o titular mais fraco fica refém do sistema.

Por outro lado, no campo musical observa-se um cenário de remuneração por execução pública, no qual o Escritório Central de Arrecadação e Distribuição (ECAD) atua como entidade centralizadora desse sistema, realizando a cobrança e a posterior distribuição dos direitos autorais decorrentes da utilização pública de obras musicais. Assim, se, por um lado, no setor audiovisual, prevalece com frequência a lógica de remuneração única característica do modelo buyout, por outro, o sistema de gestão coletiva implementado pelo ECAD se apresenta como um mecanismo robusto, capaz de assegurar a adequada remuneração dos titulares a partir das sucessivas utilizações da obra, em proporção à sua efetiva exploração e alcance.

2. O ESCRITÓRIO CENTRAL DE ARRECADAÇÃO E DISTRIBUIÇÃO (ECAD)

O ECAD é uma instituição privada, sem fins lucrativos, que exerce o monopólio legal da gestão coletiva de direitos autorais de execução pública musical no Brasil. Instituído originalmente pela Lei nº 5.988/73 e mantido pela atual Lei de Direitos Autorais (Lei nº 9.610/98), o órgão é administrado por sete associações de gestão coletiva, são elas: Abramus, Amar, Assim, Sbacem, Sicam, Socinpro e UBC. (COELHO, 2013)

A existência de um ente centralizador é justificada pela complexidade de fiscalizar o uso individual de obras em um território vasto. Foi criado, nos termos do Art. 99 deste preceito legal, “para a arrecadação e distribuição, em comum, dos direitos relativos à execução pública das obras musicais e lítero-musicais e de fonogramas, inclusive por meio da radiodifusão e transmissão por qualquer modalidade, e da exibição de obras audiovisuais.”

A legislação impõe que qualquer usuário que deseje utilizar obras musicais publicamente deve obter autorização prévia e efetuar o pagamento dos direitos ao escritório. O descumprimento sujeita o infrator a sanções judiciais, incluindo multas que podem chegar a vinte vezes o valor devido.

A distribuição não ocorre de forma uniforme para todos os tipos de uso da música; ela é organizada em um calendário mensal que divide o repasse por segmentos de utilização. Essa organização permite que o ECAD processe o volume massivo de dados provenientes de diferentes fontes de execução pública.

De acordo com o cronograma oficial, os repasses não são imediatos, são estruturados da seguinte forma: Distribuição Mensal: O segmento de Shows é o único que possui distribuição todos os meses do ano (janeiro a dezembro). Distribuição Trimestral: A maioria dos outros segmentos segue um ciclo de quatro pagamentos anuais, agrupados por natureza de uso: Janeiro, Abril, Julho e Outubro: Rádio, Direitos Gerais, Música ao Vivo, Casas de Festas e Diversão,

Sonorização Ambiental, TV Aberta e Simulcasting. Fevereiro, Maio, Agosto e Novembro: Streaming de Áudio e Vídeo e TV por Assinatura. Março, Junho, Setembro e Dezembro: Cinema

No que tange aos valores, a Lei nº 12.853/2013 define que 10% ficam com o ECAD para despesas administrativas, 5% são destinados às associações para custear despesas operacionais e 85% são destinados aos titulares filiados às associações.

O principal ponto positivo do ECAD é a viabilização da remuneração em escala. Para um artista individual, seria humanamente impossível negociar e cobrar de milhares de rádios, restaurantes e plataformas digitais simultaneamente. Ante a esta nebulosa situação José Carlos Costa Netto traz a seguinte indagação: “Como poderá o autor autorizar, controlar o uso e receber remunerações decorrentes do aproveitamento de sua obra?”

Além disso, a jurisprudência brasileira, consolidada no STJ e STF, fortaleceu o reconhecimento do trabalho artístico ao considerar o streaming como execução pública. Isso garantiu que as novas tecnologias não se tornassem um “vácuo” de remuneração, permitindo ao ECAD cobrar taxas de plataformas como Spotify e YouTube. (DELAZERI, 2019)

2.1. Os Gargalos da Gestão Coletiva: Opacidade, Burocracia e a Crise de Legitimidade do ECAD

Um dos principais gargalos identificados na atuação do Escritório Central de Arrecadação e Distribuição (ECAD) reside na sua natureza monopolista e na centralização excessiva de todas as etapas do processo autoral. O ECAD aparece como um órgão que monopoliza e centraliza toda a arrecadação, administração e supervisão dos direitos de execução pública musical no país.

A complexidade do sistema de arrecadação e distribuição do ECAD gera o que a Análise Econômica do Direito define como assimetria de informação. Esse fenômeno ocorre quando uma das partes (neste caso, o escritório central) detém muito mais dados e

conhecimentos técnicos sobre a transação do que os próprios artistas e usuários. Essa opacidade dificulta que os titulares exerçam a atividade de acompanhamento real dos seus rendimentos. (BRANT, 2018)

Outro gargalo crítico é a dificuldade do órgão em se adaptar plenamente à era digital. Embora a Lei nº 12.853/2013 tenha trazido mudanças significativas, como a supervisão (ainda que limitada) do Ministério da Cultura, observa-se ainda não houve ampla aderência às novas tecnologias. No contexto do streaming e das novas formas de consumo imaterial, a falta de uma cláusula geral sobre usos livres e a rigidez do sistema atual dificultam o equilíbrio entre a proteção do autor e o acesso à informação.

A ineficiência operacional também se reflete nos custos do sistema. Embora a taxa administrativa tenha sido reduzida de 25% para 15% após a reforma de 2013, o montante ainda é visto como elevado, alimentando um sistema que muitos descrevem como uma imensa burocracia ineficiente e cara. Do ponto de vista econômico, esse monopólio pode gerar perdas de eficiência, resultando em preços mais altos para os usuários de música e uma remuneração que os artistas consideram insatisfatória para sua manutenção produtiva.

A percepção de falta de transparência e os critérios de cobrança considerados arbitrários por alguns setores criam um terreno fértil para o fenômeno do free rider (carona). Usuários como hotéis, motéis e academias frequentemente questionam a incidência da cobrança em suas dependências, buscando valer-se das obras protegidas sem a devida contraprestação legal. Esse comportamento caroneiro reduz a arrecadação total e desincentiva a criação de novas obras, gerando um ciclo de judicialização excessiva que engarrafa os tribunais.

As decisões judiciais têm tentado corrigir essa falha, validando as tabelas de preços e critérios do ECAD para evitar que o sistema colapse. Entretanto, a solução definitiva para esses gargalos, segundo a Análise Econômica do Direito, passaria por uma maior abertura à concorrência entre associações, transparência radical e a implementação de mecanismos tecnológicos que automatizem o processo. Nesse cenário, a inovação tecnológica surge não apenas

como um desafio, mas como o caminho necessário para superar a opacidade e garantir que cada execução musical seja convertida em pagamento direto e justo ao criador, reduzindo a necessidade de intermediários burocráticos.

3. SMART CONTRACTS

Os smart contracts oferecem um vasto leque de aplicações para superar os desafios do licenciamento e da distribuição de royalties na propriedade intelectual, promovendo um ecossistema mais dinâmico e equitativo.

Uma das aplicações mais transformadoras é a distribuição direta e automática de royalties. Os smart contracts permitem a divisão instantânea dos valores arrecadados entre todos os participantes de um projeto criativo. Por exemplo, um músico pode receber sua parte dos royalties no exato momento em que sua música é reproduzida em uma plataforma conectada à blockchain (COIN, 2025). Esse modelo aborda diretamente o problema dos pagamentos retroativos e residuais, assegurando que toda nova receita gerada por uma obra seja redistribuída automaticamente para autores, atores, músicos ou outros colaboradores (COIN, 2025; DUARTE, 2023). A rastreabilidade permanente na blockchain facilita auditorias e previne a omissão de lucros, conferindo aos artistas maior previsibilidade e autonomia em sua gestão financeira (COIN, 2025). Iniciativas como a da Warner Music Group já utilizam smart contracts para essa finalidade (COIN, 2025).

A tecnologia blockchain e os smart contracts possibilitam a realização de transações diretas entre criadores e consumidores, eliminando a dependência de intermediários centralizados que, historicamente, retêm uma parcela substancial dos lucros (DUARTE, 2023; LIMA; NETO, 2024). A autoexecução dos contratos inteligentes reduz drasticamente a burocracia, minimiza riscos de descumprimento e economiza custos de transação e cobrança (COIN, 2025; CRUZ, 2025; LIMA; NETO, 2024; MIGALHAS, s.d., “Contratos Inteligentes (Smart Contracts) e sua Validade Jurídica no Brasil”). Isso pode levar a um

aumento da margem de lucro para os artistas e à aceleração da entrega de produtos digitais (COIN, 2025). Startups brasileiras, como a Smart Rights e a LA Music, já utilizam blockchain e inteligência artificial para otimizar a certificação de direitos autorais, o registro de transações e a fiscalização de valores devidos em plataformas de streaming, agilizando o recebimento para autores e executores e reduzindo perdas (COINTELEGRAPH, 2021).

3.1. Smart Contracts e Direitos Autorais

No audiovisual, a FilmChain é um exemplo relevante da aplicabilidade dos Smart Contracts neste mercado, que se apresenta como uma plataforma para coletar, alocar e analisar receitas em filme, TV e digital, com transparência e eficiência, operando com a combinação entre smart contracts e parceiros bancários. (FILMCHAIN, 2026).

A Comissão Europeia, por meio do CORDIS, noticiou uma parceria piloto em que a FilmChain foi encarregada de gerir royalties de filmes e mencionou a sua tecnologia para gestão automatizada de royalties, o que indica uso efetivo em ambiente de mercado. (CORDIS, 2021).

Para o debate brasileiro, a FilmChain é importante por mostrar um caminho pragmático: não é necessário tokenizar tudo, nem depender de criptoativos para colher benefícios. O valor está em (i) rastrear ownership/splits; (ii) registrar receitas recebidas; e (iii) automatizar alocação e relatórios de forma auditável.

No mercado musical, iniciativas se dividem entre padrões de dados e automação de pagamentos. A OMI, liderada por Berklee, se coloca como iniciativa de protocolos abertos para identificar titulares e simplificar compensação. (OMI, 2016).

A Berklee noticiou parceria com MIT para desenvolver o RAIDAR, plataforma construída com blockchain para permitir licenciamento e monetização de música entre estudantes e, potencialmente, outros

mercados, demonstrando aplicação prática para licenciamento – incluindo usos em mídia visual. (BERKLEE, 2020).

No plano de pagamentos e splits, a documentação da Revelator descreve smart contracts que automatizam distribuição de royalties para múltiplas partes e permitem liquidação em USDC, em um produto chamado Royalty Splits. (REVELATOR, 2026).

Os casos sugerem que smart contracts são mais eficazes quando (i) as partes já concordam sobre percentuais e regras; (ii) existe fonte confiável de dados de uso/receita; e (iii) a automação reduz custos de conciliação e acelera pagamentos. Quando esses três elementos não estão presentes, o projeto tende a estagnar em provas de conceito.

Em outras palavras: o “segredo” não é o blockchain, mas a combinação de governança de direitos (splits), governança de dados (oráculos) e execução financeira (pagamento).

3.2. Internet das Coisas Musicais

A Internet das Coisas Musicais é uma forma de visualizar como a tecnologia blockchain e os smart contracts podem agir como solução disruptiva para os problemas históricos da indústria musical, como a falta de transparência, a complexidade no compartilhamento de valor e a dependência de intermediários entre o artista e o fã.

Considerando que os smart contracts são códigos descentralizados e autônomos que executam cláusulas automaticamente quando certas condições são atendidas é possível que os royalties sejam gerenciados sem a necessidade de uma entidade central. Enquanto no modelo tradicional (como o do ECAD) os pagamentos dependem de sistemas burocráticos e processos operacionais lentos e obscuros, na blockchain eles podem ser instantâneos, ocorrendo imediatamente após o consumo de uma peça musical.

A blockchain possibilita transações peer-to-peer (ponto a ponto), o que reduz a necessidade de sociedades de direitos e intermediários. No ecossistema da Internet das Coisas Musicais (IoMusT), NGO, Chan Nam. TURCHET, Luca. 2022, preveem cenários

onde o próprio instrumento identifica a música tocada e realiza o pagamento automático aos compositores através de smart contracts, eliminando a necessidade de uma sociedade mediadora para cobrar o local do evento (“Instrumentos Musicais Inteligentes”). Assim como, dispositivos equipados com inteligência podem identificar automaticamente *covers* em shows ao vivo, cruzando os dados com registros na blockchain para garantir a recompensa imediata aos compositores originais (“Identificação de Covers”)

Um dos maiores gargalos atuais é a existência de bancos de dados proprietários e fragmentados sobre a propriedade de direitos autorais. A blockchain permite a criação de um banco de dados em rede de propriedade de direitos autorais, onde as informações são atualizadas de forma automatizada, instantânea e ficam disponíveis para todos os usuários. Isso evita que receitas acabem em “caixas-pretas” onde os proprietários legítimos não podem ser identificados.

Para lidar com grandes volumes de dados (como arquivos de áudio), a blockchain utiliza o armazenamento descentralizado, mantendo na rede apenas os ponteiros (URIs) ou hashes dos arquivos, o que garante a integridade dos dados sem sobrecarregar a cadeia. Além disso, a tecnologia facilita micropagamentos com custos de transação muito mais baixos, tornando viável a monetização de cada pequena execução ou uso de dados. (NGO, TURCHET, 2022.)

Apesar do potencial, a integração entre blockchain e o mercado musical enfrenta desafios técnicos, como latência: Aplicações musicais exigem respostas em tempo real (menos de 30ms), enquanto a criação de blocos na blockchain pode ser demorada; escalabilidade: A blockchain não foi projetada para armazenar as enormes quantidades de dados geradas em tempo real por “Coisas Musicais”; questões Legais: A proteção de dados e as leis de privacidade (como a LGPD) ainda precisam ser harmonizadas com a natureza imutável da blockchain. (NGO, TURCHET, 2022.)

Em suma, a visão de uma Internet das Coisas Musicais baseada em Blockchain (BloMusT) sugere que as sociedades de direitos autorais tradicionais podem ter seu papel reduzido ou até desaparecer,

à medida que a tecnologia permite que os artistas sejam remunerados de forma justa, direta e transparente.

CONSIDERAÇÕES FINAIS

As transformações tecnológicas e econômicas analisadas ao longo deste trabalho evidenciam que a discussão sobre direitos autorais no Brasil ultrapassa a dimensão estritamente jurídica e se insere, de forma cada vez mais evidente, no campo da governança de dados, da arquitetura de sistemas e da eficiência na distribuição de valor. A comparação entre os setores musical e audiovisual demonstra que o problema central não reside na ausência de proteção normativa - que já existe de forma relativamente abrangente na Lei de Direitos Autorais, mas na forma como essa proteção se materializa economicamente para os titulares.

No campo musical, a existência de um sistema de gestão coletiva estruturado, centralizado no ECAD, viabilizou a criação de um fluxo contínuo de arrecadação e distribuição de valores decorrentes da execução pública. Trata-se de um modelo que, apesar de suas críticas, cumpre uma função essencial: transformar o uso difuso e massificado das obras musicais em remuneração efetiva para seus titulares. A lógica subjacente é a de escala - somente um ente centralizador é capaz de monitorar, cobrar e distribuir valores em um cenário de múltiplos usuários e execuções simultâneas. Ainda que marcado por desafios relevantes, como a opacidade, os custos operacionais e questionamentos quanto à sua legitimidade, o ECAD representa, na prática, um mecanismo funcional de conversão da exploração econômica em renda autoral.

Por outro lado, o setor audiovisual brasileiro revela um cenário distinto, no qual a remuneração de intérpretes e outros profissionais da cadeia criativa permanece fortemente dependente da negociação contratual individual. A predominância de cláusulas de buyout, que concentram a remuneração em pagamentos únicos, evidencia uma fragilidade estrutural: a ausência de mecanismos padronizados e

coletivos capazes de capturar e redistribuir receitas decorrentes da exploração continuada das obras. Nesse contexto, a assimetria de poder de barganha se torna determinante, frequentemente colocando os titulares em posição de vulnerabilidade e contribuindo para a recorrente judicialização do tema.

A análise comparativa permite concluir que há, no Brasil, uma assimetria institucional entre os dois setores. Enquanto a música dispõe de uma infraestrutura consolidada de gestão coletiva - ainda que imperfeita, o audiovisual carece de mecanismos equivalentes que assegurem remuneração proporcional à efetiva exploração das obras ao longo do tempo. Essa lacuna se torna ainda mais relevante diante da digitalização do consumo e da centralidade das plataformas de streaming, que ampliam exponencialmente as possibilidades de monetização, mas também tornam mais complexa a rastreabilidade dos fluxos financeiros.

É nesse contexto que as tecnologias baseadas em blockchain e os smart contracts emergem como instrumentos potencialmente capazes de reconfigurar a forma como direitos autorais são geridos e remunerados. Conforme demonstrado, o principal valor dessas tecnologias não está na substituição do contrato tradicional, mas na sua complementação por meio de automação, rastreabilidade e auditabilidade. Os chamados smart legal contracts oferecem um modelo híbrido no qual cláusulas jurídicas são combinadas com execuções automatizadas, permitindo que regras previamente acordadas - como percentuais de divisão de receitas - sejam cumpridas de forma imediata e transparente.

As experiências analisadas, como a FilmChain no audiovisual e soluções de royalty splits no mercado musical, demonstram que a aplicação prática dessas tecnologias já é uma realidade, ainda que em estágio inicial. Esses casos evidenciam que a eficiência dos smart contracts depende menos da tecnologia em si e mais da qualidade da governança que a sustenta. Em particular, três elementos se mostram essenciais: a definição clara de titularidade e percentuais (splits), a existência de fontes confiáveis de dados sobre uso e receita (oráculos)

e a capacidade de execução financeira integrada. Sem esses pilares, a automação tende a se limitar a experimentos isolados, sem impacto estrutural.

No entanto, a adoção dessas soluções no Brasil não está isenta de desafios. Do ponto de vista jurídico, questões relacionadas à validade, interpretação e responsabilização em contratos automatizados ainda demandam maior desenvolvimento doutrinário e jurisprudencial. Além disso, a compatibilização entre a imutabilidade da blockchain e os princípios da Lei Geral de Proteção de Dados impõe limites e exige soluções técnicas sofisticadas, como o uso de dados off-chain e mecanismos de anonimização. Do ponto de vista técnico, problemas de escalabilidade, latência e integração com sistemas existentes também representam obstáculos relevantes.

Outro ponto que merece destaque é que a tecnologia, por si só, não resolve problemas estruturais de mercado. A simples implementação de blockchain ou smart contracts não elimina assimetrias de poder, nem garante automaticamente uma distribuição mais justa de receitas. Ao contrário, há o risco de que novas infraestruturas reproduzam desigualdades já existentes, caso não sejam acompanhadas de diretrizes regulatórias e institucionais adequadas. Nesse sentido, a discussão sobre inovação tecnológica deve necessariamente caminhar em conjunto com o debate sobre regulação e políticas públicas.

Diante desse cenário, este trabalho propõe que o caminho mais promissor para o Brasil não está na substituição de modelos existentes, mas na sua evolução. No caso do ECAD, isso significa avançar em direção a maior transparência, eficiência operacional e incorporação de tecnologias que permitam auditoria em tempo real e melhor rastreabilidade dos usos. No audiovisual, por sua vez, a criação de mecanismos híbridos - que combinem negociação contratual com automação de pagamentos e registro de dados - pode representar um avanço significativo na garantia de remuneração proporcional aos titulares.

Adicionalmente, iniciativas regulatórias em discussão no país, como a previsão de remuneração residual para obras audiovisuais

no ambiente digital, indicam que há um movimento institucional em curso. A incorporação de soluções tecnológicas nesse processo pode não apenas viabilizar a implementação dessas políticas, mas também aumentar sua eficiência e reduzir custos de fiscalização e execução.

Por fim, é possível afirmar que o futuro da remuneração na economia criativa dependerá, em grande medida, da capacidade de integração entre direito e tecnologia. A construção de sistemas mais justos, transparentes e eficientes exige não apenas inovação técnica, mas também um redesenho das estruturas institucionais e contratuais que sustentam o mercado. Nesse contexto, os smart contracts devem ser compreendidos não como uma solução isolada, mas como parte de um ecossistema mais amplo de transformação.

Em síntese, a principal contribuição deste trabalho reside em evidenciar que a discussão sobre direitos autorais no Brasil não pode mais se limitar ao plano normativo ou contratual tradicional. A emergência de novas tecnologias impõe a necessidade de repensar modelos de governança, distribuição de receitas e proteção de direitos. Ao aproximar as experiências do mercado musical e audiovisual e explorar o potencial dos smart contracts, buscou-se demonstrar que há caminhos concretos para reduzir assimetrias, aumentar a eficiência e, sobretudo, assegurar que a exploração econômica das obras criativas se traduza, de forma mais justa e proporcional, na remuneração de seus titulares.

REFERÊNCIAS

BERKLEE COLLEGE OF MUSIC. Berklee partners with MIT to help students get paid for their music (RAIDAR). 2020. Disponível em: <https://college.berklee.edu/news/berklee-now/berklee-partners-mit-help-students-get-paid-their-music>.

BRANT, Leonardo Brant. Direito Autoral e Direitos Conexos. 7. Ed. Rio de Janeiro: Forense, 2018.

BRASIL. Lei nº 9.610, de 19 de fevereiro de 1998. Altera, atualiza e consolida a legislação sobre direitos autorais. Disponível em: https://www.planalto.gov.br/ccivil_03/Leis/L9610.htm.

CISAC. Guidelines on Copyright Buyouts. Disponível em: <https://members.cisac.org/CisacPortal/cisacDownloadFileSearch.do?docId=39884&lang=en>.

COELHO, Fábio Ulhoa. Curso de direito civil, volume 4: direito das coisas, direito autoral. 5. Ed. São Paulo: Saraiva, 2013.

COIN, Sabrina. Como contratos inteligentes estão mudando arte, música e mídia. Blocknews, [S. l.], 13 jun. 2025.

COINTELEGRAPH. Startups brasileiras de música revolucionam mercado de direitos autorais com blockchain. [S. l.], 20 jan. 2021.

CORDIS (European Commission). Getting royalties to film content creators (FilmChain). 2021. Disponível em: <https://cordis.europa.eu/article/id/435842-getting-royalties-to-film-content-creators>.

CRUZ, Pedro. Contratos Inteligentes e Blockchain. Franco de Menezes Advogados, [S. l.], 25 mar. 2025.

DELAZERI, Diego. O entendimento do Recurso Especial n. 1559.264/RJ nos casos de execução pública na tecnologia streaming. JusBrasil,

7 fev. 2019. Disponível em: [Direitos autorais na execução pública de conteúdo via streaming - Jus.com.br | Jus Navigandi](#)

DUARTE, Allan Coelho. A propriedade intelectual na era da Web 3.0: como a blockchain, os smart contracts e os NFTs podem afetar os direitos de autor. 2023. 141 f. Dissertação (Mestrado Acadêmico em Direito Constitucional) – Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, Brasília, 2023.

FERRO, Enrico; SALTARELLA, Marco; ROTONDI, Domenico; GIOVANELLI, Marco; CORRIAS, Giacomo; MONCADA, Roberto; CAVALLARO, Andrea; FAVENZA, Alfredo. Digital assets rights management through smart legal contracts and smart contracts. Blockchain: Research and Applications, v. 4, n. 3, 2023, 100142. DOI: 10.1016/j.bcr.2023.100142. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2096720923000179>.

FILMCHAIN. FilmChain – collect, allocate and analyse revenues in film, TV and digital. Disponível em: <https://filmchain.co/>.

LEAL, Leonardo José Peixoto; ROCHA, Maria Val da Rocha. Direitos da personalidade e a proteção do conteúdo patrimonial dos direitos autorais. RIDB, ano 3, n. 9, 2014, p. 6969 e 6970, Disponível em www.idb-fdul.com

MIGALHAS. Contratos Inteligentes (Smart Contracts) e sua Validade Jurídica no Brasil. [S. l.]: Migalhas, [s.d.].

MIT DIGITAL CURRENCY INITIATIVE (MIT DCI). Blockchain rights management with the Open Music Initiative. 2016. Disponível em: <https://www.dci.mit.edu/posts/blockchain-rights-management-with-the-open-music-initiative>.

NETTO, José Carlos Costa. Direito autoral no Brasil. São Paulo: FTD, 1998.

NGO, Chan Nam. TURCHET, Luca. 2022. Blockchain-based Internet of Musical Things. Disponível em: <https://pdf.sciencedirectassets.com>

OPEN MUSIC INITIATIVE (OMI). Open Music Initiative (site institucional). Disponível em: <https://open-music.org/>.

REVELATOR. Royalty Splits (documentação). Disponível em: <https://docs.revelator.com/pro/platform/royalties/royalty-splits>.

SENADO FEDERAL. Projeto garante remunerar obra audiovisual executada na internet (PL 4.968/2024). 2025. Disponível em: <https://www12.senado.leg.br/noticias/materias/2025/01/22/projeto-garante-remunerar-obra-audiovisual-executada-na-internet>.

3. DA INVIABILIDADE TÉCNICA À CONFORMIDADE REGULATÓRIA: UM ESTUDO SOBRE BLOCKCHAIN E CRIPTOGRAFIA APLICADA À PROTEÇÃO DE DADOS PESSOAIS

Davi Wainer Costa

Especialista em Direito Digital pelo Instituto de Tecnologia e Sociedade do Rio de Janeiro – ITS Rio em parceria com o Centro de Estudos e Pesquisas no Ensino do Direito da Universidade do Estado do Rio de Janeiro (CEPED/ UERJ).

1. INTRODUÇÃO

A ascensão de tecnologias disruptivas como a blockchain tem provocado debates intensos acerca da compatibilidade entre inovação tecnológica e os marcos regulatórios contemporâneos de proteção de dados. Embora a descentralização, a transparência e a imutabilidade dos registros se apresentem como virtudes que asseguram a integridade e a confiabilidade das transações digitais, esses mesmos atributos acabam colidindo com normas jurídicas garantidoras de direitos fundamentais, em especial o direito à proteção de dados pessoais. No Brasil, esse direito foi positivado pela Lei nº 13.709/2018, a Lei Geral de Proteção de Dados Pessoais (LGPD); e, em nível europeu, pelo Regulamento Geral sobre Proteção de Dados (GDPR), que se consolidaram como paradigmas regulatórios sobre o tema.

O ponto de maior tensão entre blockchain e proteção de dados reside na característica de imutabilidade: uma vez inseridas, as informações não podem ser modificadas ou excluídas da rede sem comprometer a integridade do sistema. Essa propriedade contrasta diretamente com os dispositivos legais que asseguram ao titular o direito de eliminação ou, em termos mais amplos, o direito ao esquecimento. A aplicação estrita da legislação a ecossistemas descentralizados e inalteráveis pode, portanto, levar a impasses de

difícil solução, seja pela inviabilidade técnica da exclusão, seja pela ausência de um agente de tratamento claramente identificado como responsável no ambiente distribuído⁵¹.

Esse contexto suscita a necessidade de investigação sobre métodos técnicos capazes de mitigar o conflito entre inovação e regulação, de modo a preservar tanto os valores jurídicos de proteção da personalidade quanto a funcionalidade tecnológica da blockchain. O presente trabalho parte dessa problemática e tem como objetivo central analisar métodos criptográficos como alternativas conciliatórias para compatibilizar a imutabilidade dos registros com as exigências de exclusão de dados previstas em legislações de proteção de dados pessoais.

A relevância do estudo se manifesta em duas frentes. De um lado, no plano jurídico, contribui para o debate ainda incipiente sobre a aplicação da LGPD a sistemas distribuídos e imutáveis, oferecendo parâmetros para a atuação de reguladores, tribunais e agentes de tratamento. De outro lado, no plano técnico, permite compreender as possibilidades e limitações dos métodos criptográficos disponíveis, apontando caminhos para soluções práticas como funções hash e *commitments*, armazenamento *off-chain*, chaves rotativas e *crypto-shredding*, criptografia homomórfica, provas de conhecimento zero (*zero-knowledge proofs*), *pruning* e *chameleon hashes*.

Metodologicamente, adota-se a pesquisa bibliográfica e documental, com análise de obras doutrinárias, artigos científicos recentes, relatórios de organismos internacionais e documentos regulatórios. A pretensão do presente trabalho é de delimitar as principais alternativas técnicas atualmente discutidas, avaliando sua viabilidade jurídica à luz da LGPD e do GDPR. O recorte está centrado no estudo da blockchain pública e não-permissionada, considerando-se que nesses modelos a questão da exclusão de dados apresenta maior complexidade, em razão da ausência de governança centralizada e da ampla replicação dos registros.

51 FLORIAN, Martin et al. *Erasing Data from Blockchain Nodes*. In: IEEE European Symposium on Security and Privacy Workshops. IEEE, 2019. p. 9. Disponível em: Link. Acesso em: 7 ago. 2025.

2. FUNDAMENTOS MÍNIMOS DA BLOCKCHAIN

A blockchain é uma tecnologia de registro distribuído (*Distributed Ledger Technology – DLT*) que se caracteriza pela descentralização, pela imutabilidade e pela segurança dos dados nela armazenados. Diferentemente dos bancos de dados tradicionais, que dependem de uma autoridade central para validação e controle, a blockchain funciona por meio de uma rede de nós (*nodes*) interconectados, responsáveis por validar e armazenar, de forma consensual, as informações registradas. Esse modelo promove maior transparência, elimina a necessidade de intermediários e fortalece a confiança entre partes que não possuem relação prévia de credibilidade recíproca⁵².

A descentralização é um dos pilares da tecnologia. Em sistemas centralizados, a integridade dos registros depende de um único agente, que atua como intermediário confiável. Tal panorama, embora eficiente em muitos contextos, gera vulnerabilidades, uma vez que falhas ou ataques ao ponto central podem comprometer toda a rede. Na blockchain, por sua vez, cada nó mantém uma cópia integral do histórico de transações, o que garante resiliência e dificulta manipulações indevidas⁵³. Quanto maior o número de nós participantes, mais robusta se torna a rede, dificultando tentativas de adulteração e fortalecendo a integridade do sistema.

Outro atributo fundamental é a imutabilidade. Cada bloco da cadeia contém um conjunto de transações validadas, bem como um identificador criptográfico (*hash*) do bloco anterior. Essa estrutura encadeada implica que qualquer alteração em um dado bloco modificaria automaticamente todos os blocos subsequentes, o que tornaria imediatamente detectável a fraude. Em blockchains públicas, de elevada descentralização, essa característica inviabiliza, na prática,

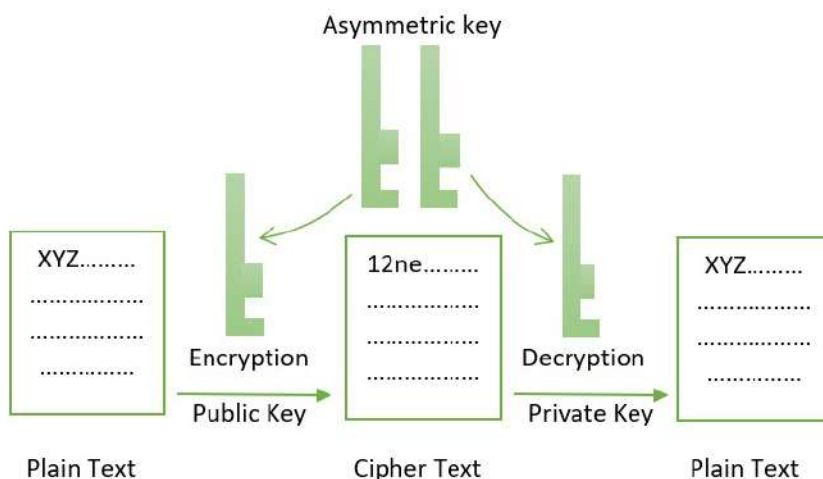
52 CASEY, Michael et al. *The Impact of Blockchain Technology on Finance: A Catalyst for Change*. Geneva: ICMB, 2018, p. 14. Disponível em: Link. Acesso em: 7 ago. 2025.

53 ABROL, Ayushi. Blockchain vs. Distributed Ledger Technology. *Blockchain Council*, 2018. Disponível em: Link. Acesso em: 7 ago. 2025.

a exclusão ou alteração de registros, motivo pelo qual afirma-se que tais sistemas são *append-only* (apenas aditivos)⁵⁴.

A segurança da rede, por sua vez, decorre diretamente da aplicação de métodos criptográficos. Duas técnicas são centrais: (i) a criptografia assimétrica, baseada no uso de pares de chaves pública e privada, que assegura a identidade dos usuários e a confidencialidade das transações; e (ii) as funções hash, que transformam entradas de dados de qualquer tamanho (como um arquivo, texto ou senha) em cadeias alfanuméricas de comprimento fixo, servindo para validar a integridade dos registros e impedir adulterações. Pequenas alterações no dado de entrada geram um hash completamente distinto, permitindo identificar manipulações mesmo que mínimas⁵⁵. A lógica da criptografia assimétrica pode ser visualizada na **Figura 1**, enquanto a função hash é exemplificada na **Figura 2**, ambas essenciais para compreender os mecanismos de segurança da blockchain.

Figura 1 – Representação da criptografia assimétrica

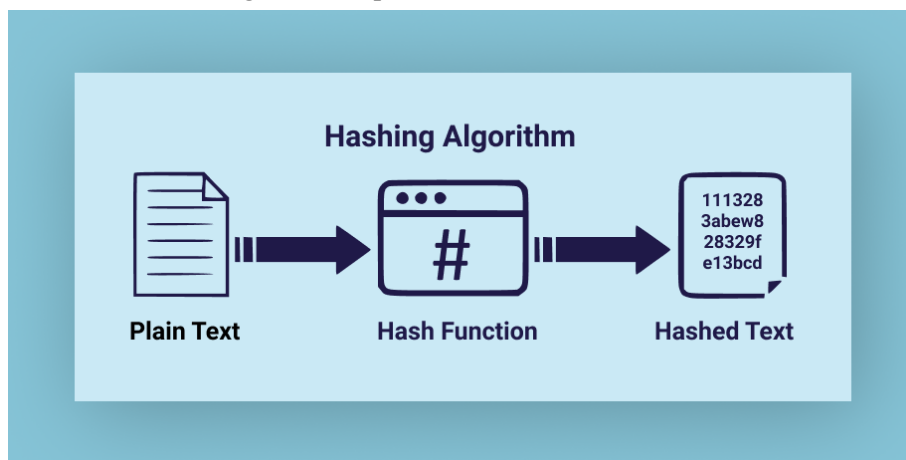


Fonte: Adaptado de GeeksforGeeks (2025).

54 TAPSCOTT, Don; TAPSCOTT, Alex. *Realizing the Potential of Blockchain*. World Economic Forum, 2017, p. 5. Disponível em: Link. Acesso em: 7 ago. 2025.

55 LIN, Iuon-Chang; LIAO, Tzu-Chun. A Survey of Blockchain Security Issues and Challenges. *International Journal of Network Security*, v. 19, n. 5, p. 653–659, 2017. Disponível em: Link. Acesso em: 7 ago. 2025.

Figura 2 – Representação da função hash



Fonte: Adaptado de Medium (2021).

Além da criptografia, a validação dos registros depende de mecanismos de consenso, que permitem que todos os nós concordem quanto ao estado da rede. Entre os mais utilizados, destacam-se o *proof of work* (PoW) e o *proof of stake* (PoS). O primeiro, consagrado pela rede Bitcoin, baseia-se na resolução de problemas matemáticos complexos pelos mineradores, que são recompensados pela inclusão de novos blocos. Essa técnica, embora eficiente para a segurança, é criticada pelo elevado consumo energético⁵⁶. Já o PoS, utilizado mais recentemente pela rede Ethereum, substitui o poder computacional pela quantidade de ativos detidos na rede, atribuindo maior poder de validação a quem possui mais moedas. Tal modelo reduz o gasto energético e favorece a escalabilidade, mas não elimina todos os riscos de concentração de poder econômico⁵⁷.

Esses fundamentos técnicos explicam tanto o potencial transformador da blockchain quanto as dificuldades em compatibilizá-la com a legislação de proteção de dados. A imutabilidade, que

⁵⁶ NAKAMOTO, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008. Disponível em: Link. Acesso em: 7 ago. 2025.

⁵⁷ CASTOR, Amy. Why Ethereum is switching to proof of stake and how it will work. *MIT Technology Review*, 2022. Disponível em: Link. Acesso em: 7 ago. 2025.

garante segurança e integridade, cria entraves quando confrontada com direitos fundamentais como o direito de exclusão de dados pessoais. Essa tensão será explorada nos capítulos seguintes, quando se discutir os métodos criptográficos como alternativas para conciliar a permanência dos registros e a exigência jurídica de eliminação.

A análise dos fundamentos técnicos da blockchain demonstra que sua principal virtude, a imutabilidade dos registros, também constitui o seu maior desafio jurídico. Se por um lado a imutabilidade garante segurança, confiabilidade e resistência a fraudes, por outro ela colide com as exigências normativas que asseguram aos titulares de dados pessoais o direito de solicitar sua exclusão ou anonimização. Surge, assim, um ponto de fricção entre a tecnologia e o direito: a impossibilidade prática de apagar dados registrados em uma rede distribuída pode comprometer a efetividade de garantias fundamentais previstas em legislações como a LGPD e o GDPR.

A partir desse contraste, torna-se necessário examinar com mais profundidade os contornos jurídicos da proteção de dados pessoais e os direitos assegurados pelos marcos regulatórios, para então avaliar as alternativas técnicas propostas pela comunidade científica e jurídica como formas de conciliação.

A POSITIVAÇÃO DO DIREITO À PROTEÇÃO DE DADOS PESSOAIS

A centralidade da informação na sociedade contemporânea conferiu aos dados pessoais o *status* de insumo estratégico. A utilização de informações sobre hábitos, preferências e comportamentos passou a influenciar não apenas práticas de consumo, mas também decisões políticas e econômicas. Nesse cenário, consolidou-se o entendimento de que a proteção de dados não é apenas uma questão de privacidade

individual, mas também de garantia da autodeterminação informativa e da dignidade da pessoa humana⁵⁸.

O movimento internacional de proteção de dados teve como marco fundamental a edição do Regulamento Geral sobre a Proteção de Dados (GDPR), aprovado pela União Europeia em 2016 e aplicável a partir de 2018. O regulamento instituiu princípios como finalidade, minimização, proporcionalidade, transparência e *accountability* (prestação de contas), estabelecendo ainda um rol de direitos fundamentais dos titulares. Entre esses direitos, destaca-se o direito ao apagamento (*right to erasure*), previsto em seu art. 17, também conhecido como direito ao esquecimento. Tal prerrogativa confere ao titular a possibilidade de exigir a eliminação de seus dados pessoais quando não mais necessários para as finalidades originais, quando houver revogação do consentimento ou em caso de tratamento ilícito⁵⁹.

No Brasil, a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), inspirada no modelo europeu, introduziu um sistema semelhante de garantias. O art. 18, inciso VI, assegura ao titular o direito de solicitar a eliminação dos dados pessoais tratados com base em seu consentimento. Embora a legislação brasileira não empregue a expressão “direito ao esquecimento”, a formulação aproxima-se da lógica do GDPR, impondo ao controlador a obrigação de eliminar dados quando esgotada a base legal que fundamentava o tratamento⁶⁰.

A LGPD também delimita os papéis dos agentes de tratamento, estabelecendo a figura do controlador, responsável por tomar as decisões sobre o tratamento, e do operador, incumbido de realizá-lo em nome do controlador. Ambos respondem solidariamente por danos

58 DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. 2. ed. São Paulo: Thomson Reuters Brasil, 2019, p. 35-36.

59 VOIGT, Paul; VON DEM BUSSCHE, Axel. *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Cham: Springer, 2024, p. 202. Disponível em: Link. Acesso em: 9 ago. 2025.

60 BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: Link. Acesso em: 9 ago. 2025.

decorrentes do tratamento irregular e estão sujeitos a princípios como segurança, prevenção e responsabilização⁶¹.

Contudo, a aplicação desses conceitos ao ambiente da blockchain encontra desafios significativos. A ausência de uma autoridade central dificulta a identificação de quem seria o controlador e quem atuaria como operador. Em redes públicas e não-permissionadas (*permissionless*), todos os nós armazenam cópias integrais dos registros, o que fragmenta e dilui responsabilidades. Ademais, a imutabilidade da blockchain contrasta diretamente com o direito à exclusão de dados pessoais, tornando inviável, sob a ótica técnica, a aplicação literal das normas jurídicas que impõem o dever de apagamento⁶².

A doutrina ainda debate se técnicas como anonimização ou pseudonimização seriam suficientes para afastar a incidência da LGPD. Autores ressaltam que, se houver a possibilidade de reidentificação, mesmo indireta, os dados permanecerão sob o manto da proteção jurídica⁶³. No contexto europeu, o European Data Protection Board (EDPB) já reconheceu a existência de tensões significativas entre a tecnologia e o GDPR, em especial quanto ao direito de exclusão de dados pessoais⁶⁴. No Brasil, a Autoridade Nacional de Proteção de Dados (ANPD) ainda não expediu diretrizes específicas, o que reforça a importância de estudos acadêmicos sobre o tema.

Assim, a análise da LGPD à luz da blockchain revela não apenas um conflito aparente entre direitos fundamentais e inovação tecnológica, mas também a necessidade de compreender os pontos exatos de fricção entre os marcos regulatórios e a arquitetura técnica da tecnologia. É nesse contexto que se destaca a tensão entre a

61 SCHREIBER, Anderson. *Tratado de Direito Civil: responsabilidade civil*. São Paulo: Atlas, 2020, p. 272.

62 FINCK, Michèle. *Blockchain Regulation and Governance in Europe*. Cambridge: Cambridge University Press, 2019, p. 42. Disponível em: Link. Acesso em: 9 ago. 2025.

63 SOLOVE, Daniel J. *Understanding Privacy*. Cambridge: Harvard University Press, 2008, p. 117. Disponível em: Link. Acesso em: 9 ago. 2025.

64 FINCK, Michèle. *Blockchain and the General Data Protection Regulation*. European Parliamentary Research Service (EPRS), 2019. **Executive summary** (passagens iniciais) e **The tension between blockchain and the GDPR** (abertura da seção). Disponível em: Link. Acesso em: 9 ago. 2025.

imutabilidade da blockchain e o direito à exclusão de dados pessoais, cuja análise detalhada será realizada no próximo capítulo.

3. INCOMPATIBILIDADE ENTRE BLOCKCHAIN E A EXCLUSÃO DE DADOS PESSOAIS

Como visto anteriormente, tanto o GDPR quanto a LGPD asseguram ao titular o direito de solicitar a exclusão de seus dados pessoais. Ocorre que essa prerrogativa acaba colidindo com a imutabilidade da blockchain, característica que impede a alteração ou remoção de registros sem comprometer a integridade da rede⁶⁵. Em blockchains públicas não permissionadas, cada transação validada é replicada por todos os nós, o que torna inviável o atendimento a pedidos de exclusão⁶⁶.

O problema é agravado pela indefinição quanto aos agentes de tratamento. Enquanto a LGPD e o GDPR pressupõem a existência de um controlador responsável pelas decisões sobre o tratamento, na blockchain essa figura é difusa, já que todos os nós participam da validação e armazenam cópias dos dados. O Relatório do Serviço de Pesquisa do Parlamento Europeu aponta que a descentralização da tecnologia desafia diretamente a lógica do GDPR, tornando a alocação de responsabilidades “onerosa” e, em alguns casos, inviável⁶⁷.

Há ainda controvérsia quanto à natureza dos dados armazenados. Parte dos desenvolvedores sustenta que hashes ou identificadores criptográficos não configurariam dados pessoais. Contudo, parcela significativa da doutrina defende que, quando houver possibilidade de

65 TAPSCOTT, Don; TAPSCOTT, Alex. *Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World*. New York: Penguin, 2016, p. 72.

66 DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. 2. ed. São Paulo: Thomson Reuters Brasil, 2019, p. 231.

67 FINCK, Michèle. *Blockchain and the General Data Protection Regulation*. European Parliamentary Research Service (EPRS), 2019. **Executive summary** (passagens iniciais) e **The tension between blockchain and the GDPR** (abertura da seção). Disponível em: Link. Acesso em: 9 ago. 2025.

reidentificação indireta, tais registros devem ser considerados dados pessoais para fins de aplicação da lei⁶⁸.

Reguladores corroboram essa perspectiva crítica. O Article 29 Working Party aponta que a característica da imutabilidade pode entrar em conflito direto com direitos fundamentais, como retificação e exclusão de dados. Além disso, ressalta que a descentralização da blockchain intensifica as dificuldades de conformidade e que, para não considerar esses hashes ou identificadores criptográficos como dados pessoais, o risco de identificação⁶⁹ deve ser zero. No Brasil, a Autoridade Nacional de Proteção de Dados (ANPD) ainda não emitiu diretrizes específicas, o que amplia a insegurança jurídica para projetos que utilizam blockchain em contextos envolvendo dados pessoais.

Assim, a incompatibilidade entre blockchain e normas de proteção de dados não decorre apenas da letra da lei, mas de limitações técnicas estruturais. Esse cenário reforça a necessidade de investigar métodos alternativos que se utilizam de técnicas criptográficas capazes de viabilizar a conciliação entre a inovação tecnológica da blockchain e a segurança jurídica das normas de proteção de dados pessoais.

4. MÉTODOS CRIPTOGRÁFICOS COMO ALTERNATIVAS PARA CONCILIAÇÃO ENTRE O DIREITO À EXCLUSÃO DE DADOS PESSOAIS E A IMUTABILIDADE DA TECNOLOGIA BLOCKCHAIN

O debate sobre a compatibilidade entre a imutabilidade das blockchains e o direito fundamental à exclusão de dados pessoais evidencia um desafio que transcende o âmbito jurídico, estando interligado à estrutura técnica dessas redes. Tanto o GDPR quanto a LGPD estabelecem normas de proteção de dados que exigem

68 SCHWARTZ, Paul; SOLOVE, Daniel. *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*. Harvard Law Review, v. 86, 2011, p. 1814–1892. Disponível em: Link. Acesso em: 10 ago. 2025.

69 ARTICLE 29 WORKING PARTY. *Opinion 04/2007 on the concept of personal data (WP 136) 01248/07/EN*, 21. p. 17-20. Disponível em: Link. Acesso em: 25 ago. 2025.

mecanismos aptos a garantir que os titulares de dados possam cumprir seus direitos de retificação, anonimização e eliminação de seus dados pessoais. Por outro lado, as blockchains, principalmente as públicas e não permissionadas, foram projetadas para assegurar integridade e imutabilidade por meio da replicação e do consenso distribuído, tornando difícil a modificação retroativa de blocos sem afetar a confiança em todo o sistema⁷⁰.

Nesse contexto, a literatura especializada e várias entidades reguladoras destacam que a solução não está em tentar adaptar a blockchain ao modelo convencional de exclusão de dados, mas sim em desenvolver métodos criptográficos que reinterpretem o conceito de exclusão sob uma perspectiva técnica⁷¹. A exclusão, nesse cenário, não implicaria a eliminação física de registros, fato que seria incompatível com a natureza imutável da rede. Em vez disso, significaria tornar o dado inutilizável, indecifrável ou desvinculado de sua referência pessoal. Dessa forma, a conformidade com os princípios de proteção de dados seria obtida por meio da mitigação técnica dos riscos, mantendo, concomitantemente, a transparência e a auditabilidade inerentes às blockchains.

Essa perspectiva técnica corresponde à aplicação prática do *privacy by design*, previsto no artigo 25 do GDPR e no § 2º do artigo 46 da LGPD, que exige a incorporação de medidas de segurança e privacidade desde a concepção do sistema⁷². No caso da blockchain, trata-se de desenvolver redes que conciliem os valores de integridade, transparência e descentralização, típicos da tecnologia, com os direitos

70 FINCK, Michèle. *Blockchain and the General Data Protection Regulation*. European Parliamentary Research Service (EPRS), 2019. p. 11-13. Disponível em: Link. Acesso em: 25 ago. 2025.

71 DE FILIPPI, Primavera; WRIGHT, Aaron. *Blockchain and the Law: The Rule of Code*. Cambridge: Harvard University Press, 2018. p. 182-188. Disponível em: Link. Acesso em: 25 ago. 2025.

72 BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: Link. Acesso em: 5 set. 2025.

individuais à privacidade e ao controle informacional⁷³. As soluções propostas pela comunidade científica e por organismos internacionais têm se concentrado no uso de ferramentas criptográficas avançadas, como funções *hash* e *commitments*, chaves rotativas e *crypto-shredding*, criptografia homomórfica, provas de conhecimento zero (*Zero-Knowledge Proofs*) e modelos híbridos de armazenamento *off-chain*.

Tais mecanismos não eliminam a tensão entre imutabilidade e exclusão, mas oferecem caminhos de conciliação funcional, permitindo que o tratamento de dados pessoais em blockchain observe os princípios da minimização, finalidade e segurança. A Comissão Europeia e o European Data Protection Board (EDPB) têm destacado que o emprego dessas técnicas pode mitigar riscos de não conformidade, desde que acompanhado de avaliações de impacto à proteção de dados (DPIAs) e governança criptográfica adequada⁷⁴.

No Brasil, embora o tema ainda careça de regulamentação específica, a Autoridade Nacional de Proteção de Dados (ANPD) vem reconhecendo a importância da adoção de soluções tecnológicas preventivas e de boas práticas de anonimização e criptografia⁷⁵, e poderá reforçar suas ações e recomendações com a transformação da autarquia em uma agência reguladora, com a publicação da Medida Provisória 1317/2025. A ANPD se transforma em Agência Nacional de Proteção de Dados e passa a contar com autonomia funcional, técnica, administrativa e financeira, quadro de servidores próprios e instrumentos mais claros de poder de polícia.

Nos tópicos seguintes, serão examinadas as principais técnicas criptográficas que vêm sendo debatidas como instrumentos de harmonização entre os pressupostos da proteção de dados pessoais

73 EUROPEAN DATA PROTECTION BOARD (EDPB). *Guidelines 02/2025 on the processing of personal data through blockchain technologies*. Bruxelas: EDPB, 2025. Disponível em Link. Acesso em: 5 set. 2025.

74 Ibid. Seção 4 – *Evaluating blockchain-based processing*.

75 AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). *Estudo Preliminar sobre Anonimização e Pseudonimização para a proteção de dados pessoais*. Brasília: ANPD, 2023. p. 6-9. Disponível em: Link. Acesso em: 5 set. 2025.

e os fundamentos estruturais da blockchain, analisando-se seus aspectos técnicos, aplicabilidade prática e enquadramento jurídico.

5. FUNÇÕES HASH, COMMITMENTS E ARMAZENAMENTO *OFF-CHAIN

As funções hash criptográficas são um dos pilares essenciais da segurança da informação em sistemas distribuídos, pois permitem verificar a integridade dos dados e garantir a imutabilidade dos registros. Como Stallings⁷⁶ explica, as funções hash são algoritmos que convertem uma entrada de tamanho variável em uma sequência binária de comprimento fixo, conhecida como *digest*. Dessa forma, pequenas mudanças na entrada resultam em saídas totalmente diferentes. Essa propriedade, conhecida como resistência à preimage (pré-imagem), combinada com a resistência à colisão, assegura que seja computacionalmente impraticável reconstruir o dado original ou identificar duas entradas diferentes que produzam o mesmo hash.

Em contextos de blockchain, essas características são utilizadas tanto na sequência dos blocos quanto na confirmação da integridade dos dados registrados. No entanto, o uso do hash como meio de “anonimização” é inadequado para atender às exigências das leis de proteção de dados. Isso acontece porque o hash simples, quando usado em dados de baixa entropia, como CPF, RG ou endereço, possibilita tentativas de reidentificação por meio de ataques de dicionário ou força bruta. Como resultado, esses registros continuam sendo considerados dados pessoais.⁷⁷ Ainda nessa seara, a doutrina e as autoridades de proteção de dados concordam que o uso de funções

76 STALLINGS, William. *Cryptography and Network Security: Principles and Practice*. 5. ed. New York: Pearson, 2010. p. 329–353. Disponível em: Link. Acesso em: 27 set. 2025.

77 SCHWARTZ, Paul; SOLOVE, Daniel. *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*. Harvard Law Review, v. 86, 2011, p. 1814–1892. Disponível em: Link. Acesso em: 27 set. 2025.

hash, sem métodos adicionais de ocultamento, não é adequado para eliminar a natureza pessoal da informação⁷⁸.

A utilização de *commitment schemes* é abordada como uma alternativa mais aprimorada, pois permite que um agente “assuma um compromisso” com uma declaração ou valor específico sem divulgá-lo imediatamente. A partir do dado e de uma aleatoriedade, o emissor cria um *commitment* (compromisso) e, em um momento posterior, pode “abrir” esse compromisso ao revelar o valor e o parâmetro utilizados, demonstrando a correspondência. Em sentido figurativo, é como colocar uma carta dentro de um envelope lacrado e entregá-lo ao destinatário. Esse mecanismo mantém simultaneamente as propriedades de ocultamento⁷⁹ (*hiding*) e vinculação (*binding*), assegurando que o emissor não possa modificar o valor posteriormente e que o verificador não consiga deduzir o conteúdo antes da abertura⁸⁰.

No âmbito da harmonização entre blockchain e segurança de dados, as funções hash e os *commitments* são empregados para garantir a integridade de dados guardados fora da cadeia (*off-chain*). Ao invés de registrar informações pessoais diretamente na blockchain, o sistema armazena apenas o hash ou o compromisso criptográfico, preservando o conteúdo original em um ambiente controlado e que segue políticas de exclusão, conforme o GDPR e a LGPD. Essa abordagem diminui consideravelmente a exposição de dados pessoais

78 EUROPEAN DATA PROTECTION BOARD (EDPB). *Guidelines 02/2025 on the processing of personal data through blockchain technologies*. Bruxelas: EDPB, 2025. Disponível em Link. Acesso em: 27 set. 2025.

79 Um esquema é oculto se o compromisso não revela nenhuma informação sobre o valor comprometido antes de ser aberto, enquanto é vinculativo se o responsável pelo compromisso não puder alterar o valor ou abrir o compromisso com um valor diferente do originalmente comprometido. É impossível que um esquema seja perfeitamente (computacionalmente ilimitado) oculto e vinculado ao mesmo tempo. Ver mais em: BING, Zeng; LIANG, Cheng; XUEMING, Tang. *A Perfectly Binding Commitment Scheme Against Quantum Attacks*. Cryptology Archive, s.d. Disponível em: Link. Acesso em: 28 set. 2025.

80 PEDERSEN, Torben. *Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing*. In: *Advances in Cryptology – CRYPTO ’91*. Springer, 1992. p. 129–140. Disponível em: Link. Acesso em: 28 set. 2025.

na estrutura imutável e, em teoria, permite a exclusão do conteúdo original sem afetar a integridade dos registros *on-chain*⁸¹.

Órgãos reguladores europeus, como o European Parliamentary Research (EPRS), aconselham enfaticamente que dados pessoais sejam armazenados fora da blockchain (*off-chain*) e apenas mencionados na blockchain por meio de *hash-pointers* ou compromissos ocultantes. De acordo com o órgão, essa arquitetura técnica não elimina o tratamento de dados pessoais, mas simplifica a conformidade com os direitos de retificação e exclusão⁸², já que o tratamento principal acontece em um ambiente controlado.

Embora haja vantagens, o uso de *hashes* e *commitments* não soluciona completamente o problema da exclusão de dados em redes públicas e imutáveis. Primeiramente, a eliminação do dado *off-chain* não remove sua âncora criptográfica da cadeia. Em segundo lugar, o compromisso ainda pode ser um identificador, possivelmente relacionado a outros registros públicos, o que requer a implementação de medidas adicionais de proteção, como o uso de *salts*, chaves secretas e políticas e diretrizes de governança criptográfica⁸³. Assim, essas técnicas devem ser vistas como mecanismos de mitigação, não de eliminação, integrando-se ao princípio de *privacy by design* e de minimização de dados, em vez de serem consideradas uma solução definitiva para o direito de exclusão.

6. CHAVES ROTATIVAS E *CRYPTO-SHREDDING

Uma das opções mais promissoras para garantir o direito de exclusão de dados pessoais, mantendo a imutabilidade dos registros

81 FINCK, Michèle. *Blockchain and the General Data Protection Regulation*. European Parliamentary Research Service (EPRS), 2019. p. 29-32. Disponível em: Link. Acesso em: 28 set. 2025.

82 Ibid. p. 32.

83 BARKER, Elaine. *Recommendation for Key Management: Part 1 – General (SP 800-57, Revision 5)*. Gaithersburg, MD: National Institute of Standards and Technology (NIST), 2020. (Computer Security Resource Center – CSRC). Disponível em: Link. Acesso em 30 set. 2025.

em blockchain, é a técnica chamada *crypto-shredding* ou apagamento criptográfico. Ao contrário da exclusão física, que envolve a remoção do dado armazenado, o *crypto-shredding* impede o acesso ao conteúdo cifrado por meio da destruição permanente da chave criptográfica. Em outras palavras, o dado persiste, mas se torna incompreensível e irrecuperável, o que, sob o ponto de vista funcional, equivale à sua eliminação⁸⁴.

A lógica por trás desse método é simples: quando os dados são armazenados em formato criptografado, a chave de acesso passa a verdadeira informação sensível. Dessa forma, ao eliminar a chave de decifração, o conteúdo original é irremediavelmente perdido, ainda que os blocos permaneçam imutáveis na rede.

Em blockchains públicas e não permissionadas, o *crypto-shredding* pode ser realizado indiretamente por meio da utilização de chaves rotativas (*key rotation*). Nesse modelo, as informações pessoais não são registradas diretamente na blockchain, mas sim armazenadas de forma criptografada em rede *off-chain*, podendo ser acessadas por meio de chaves que mudam periodicamente. Quando se solicita a exclusão, as chaves correspondentes são revogadas e eliminadas, impossibilitando o acesso ao conteúdo original, mesmo que a âncora criptográfica continue registrada na blockchain. Esse modelo garante a integridade do bloco e, simultaneamente, garante a inutilização prática dos dados⁸⁵, unindo a imutabilidade técnica à finalidade jurídica da exclusão.

Do ponto de vista jurídico, a questão fundamental é determinar se a destruição da chave, tornando o dado inutilizável, pode ser considerada equivalente à eliminação exigida pelas leis de proteção de dados. Uma parte da doutrina e dos reguladores⁸⁶ concorda, desde que a operação seja irreversível e adequadamente documentada, uma

84 STALLINGS, William. *Cryptography and Network Security: Principles and Practice*. 5. ed. New York: Pearson, 2010. p. 329–353. Disponível em: Link. Acesso em: 30 set. 2025.

85 GENTRY, Craig. *A Fully Homomorphic Encryption Scheme*. Stanford University, 2009. (Tese de Doutorado). Disponível em: Link. Acesso em: 30 set. 2025.

86 ARTICLE 29 WORKING PARTY. *Opinion 05/2012 on Cloud Computing (WP 196) 01037/12/EN*, 12. p. 20-21. Disponível em: Link. Acesso em: 30 set. 2025.

vez que o dado se torna, na prática, inacessível⁸⁷ a qualquer agente de tratamento. Esse entendimento é corroborado por diretrizes internacionais, como o NIST SP 800-88 Rev.1, que considera o *cryptographic erase* um método válido de sanitização, e por relatórios europeus que enfatizam a importância das medidas técnicas na redução dos riscos de não conformidade⁸⁸.

O artigo 46, segundo a LGPD, determina que controladores e operadores devem implementar medidas de segurança para proteger os dados pessoais contra acessos não autorizados e ocorrências acidentais ou ilícitas. Apesar de o *crypto-shredding* não promover uma eliminação física, ele é considerado uma medida técnica preventiva, pois assegura que os dados não possam ser recuperados nem utilizados após o processo. Assim, sua utilização pode ser vista como alinhada ao princípio da segurança e necessidade, particularmente quando incorporada a políticas de governança de chaves e evidências de destruição documentadas em Relatórios de Impacto à Proteção de Dados Pessoais (RIPD)⁸⁹.

Não obstante, o método apresenta limitações. A principal reside na complexidade de garantir que todas as chaves derivadas ou cópias de segurança (*backups*) tenham sido igualmente destruídas, o que demanda uma governança criptográfica rigorosa e um controle estrito do ciclo de vida das chaves. Ademais, o *crypto-shredding* não soluciona a questão dos metadados públicos, como endereços de carteira, hashes de transações ou identificadores correlacionáveis, que continuam visíveis na blockchain. Assim, apesar de ser um progresso significativo, ainda é uma solução mitigatória, que precisa ser complementada com políticas de anonimização e uma arquitetura

87 FINCK, Michèle. *Blockchain and the General Data Protection Regulation*. European Parliamentary Research Service (EPRS), 2019. p. 76. Disponível em: Link. Acesso em: 30 set. 2025.

88 EUROPEAN PARLIAMENT RESEARCH SERVICE (EPRS). *Blockchain and the General Data Protection Regulation*. Bruxelas: EPRS, 2019. p. 42-43.

89 AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). *Estudo Preliminar sobre Anonimização e Pseudonimização para a proteção de dados pessoais*. Brasília: ANPD, 2023. p. 6-9. Disponível em: Link. Acesso em: 30 set. 2025.

de armazenamento híbrida para conferir maior grau de adequação às demandas normativas de proteção de dados pessoais.

7. CRIPTOGRAFIA HOMOMÓRFICA

A criptografia homomórfica se destaca entre as ferramentas criptográficas que buscam conciliar a propriedade de imutabilidade da rede com os preceitos normativos de proteção dos dados pessoais. É um método que possibilita a execução de operações matemáticas em dados cifrados, gerando resultados que, quando decifrados, equivalem exatamente ao processamento que ocorreria se os dados fossem tratados como texto simples. Em outras palavras, permite o tratamento e a análise de dados sem expor os dados originais, preservando a privacidade durante todo o ciclo de processamento⁹⁰.

O conceito remonta ao final da década de 1970, mas só se tornou viável com os avanços propostos por Craig Gentry em 2009. Ele apresentou o modelo conhecido como *Fully Homomorphic Encryption* (FHE), que permite a realização de operações de soma e multiplicação em dados cifrados⁹¹. Desde esse ponto, várias implementações têm sido criadas com o objetivo de equilibrar segurança, desempenho e compatibilidade com sistemas descentralizados. Essas técnicas possibilitam que aplicações fundamentadas em blockchain tratem dados pessoais de forma off-chain, mantendo sua integridade e auditabilidade sem comprometer o princípio da minimização de dados.

Na perspectiva prática, o uso da criptografia homomórfica constitui um tipo de “processamento confidencial”, no qual *nodes* (nós) validadores ou contratos inteligentes são capazes de realizar verificações e cálculos sem nunca acessar o conteúdo sensível. Essa

90 PAILLIER, Pascal. *Public-Key Cryptosystems Based on Composite Degree Residuosity Classes*. In: *Advances in Cryptology – EUROCRYPT '99*. Berlin: Springer, 1999. p. 223–238. Disponível em: Link. Acesso em: 30 set. 2025.

91 GENTRY, Craig. *A Fully Homomorphic Encryption Scheme*. Stanford University, 2009. (Tese de Doutorado). Disponível em: Link. Acesso em: 30 set. 2025.

particularidade a torna especialmente importante em contextos nos quais a publicidade e a transparência são demandas técnicas, porém, a confidencialidade é uma exigência legal. Ao possibilitar o cálculo em dados cifrados, a técnica diminui a probabilidade de reidentificação e permite que sistemas distribuídos cumpram os princípios de *privacy by design* e *privacy by default*, estabelecidos no artigo 25 do GDPR e no artigo 46 da LGPD⁹².

Do ponto de vista jurídico, a criptografia homomórfica é frequentemente apresentada como um meio de conciliar o dilema entre inovação e proteção de dados, pois preserva a utilidade dos registros sem revelar a identidade dos titulares. Contudo, autores alertam que seu uso não elimina totalmente o risco de violação de direitos, principalmente quando este estiver ligado a dados inferidos ou modelos de aprendizado automático que possam reconstruir informações pessoais a partir de resultados agregados⁹³. No âmbito regulatório, autoridades nacionais reconhecem que métodos de anonimização, pseudonimização e criptografia podem ser utilizados de forma complementar para diminuir os riscos de reidentificação e atenuar os efeitos do tratamento de dados pessoais⁹⁴.

No que diz respeito à implementação, ainda existem muitos desafios para o uso prático da criptografia homomórfica integral. As operações de FHE demandam um alto custo computacional e um grande volume de armazenamento, o que restringe sua utilização em blockchains de grande escala, especialmente em redes públicas e descentralizadas. Estudos recentes apontam que, embora tenha havido progressos teóricos, a implementação completa de operações

92 EUROPEAN DATA PROTECTION BOARD (EDPB). *Guidelines 02/2025 on the processing of personal data through blockchain technologies*. Bruxelas: EDPB, 2025. Disponível em Link. Acesso em: 30 set. 2025.

93 FINCK, Michèle; MOSCON, Valeria. *Copyright Law on Blockchains: Between New Forms of Rights Administration and Digital Rights Management 2.0*. JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law, v. 10, n. 1, 2019. Disponível em: Link. Acesso em: 3 out. 2025.

94 AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). *Estudo Preliminar sobre Anonimização e Pseudonimização para a proteção de dados pessoais*. Brasília: ANPD, 2023. p. 6-9. Disponível em: Link. Acesso em: 4 out. 2025.

homomórficas ainda é custosa, principalmente por causa do *bootstrapping*⁹⁵ e da necessidade de controle do ruído acumulado em operações criptográficas⁹⁶. Como alternativa, têm sido investigados modelos parciais (PHE) e limitados (SHE)⁹⁷ que possibilitam apenas operações restritas (como soma ou multiplicação), assegurando um desempenho superior com um nível de segurança considerado aceitável.

Apesar de ainda estar em fase experimental, a criptografia homomórfica se sobressai como uma ferramenta propulsora de uma blockchain juridicamente sustentável. Ela viabiliza o tratamento descentralizado de dados sensíveis, garantindo a observância dos princípios de finalidade, necessidade e segurança. Desse modo, mais do que uma técnica isolada, constitui um novo paradigma de conformidade técnica, em que o dado continua sendo útil para a rede, porém resguardado contra exposições indevidas. Trata-se de um avanço significativo na busca pela conciliação entre a dicotomia privacidade *versus* segurança jurídica em sistemas descentralizados.

8. PROVAS DE CONHECIMENTO ZERO (ZERO-KNOWLEDGE PROOFS)

As provas de conhecimento zero, ou ZKP (*Zero-Knowledge Proofs*), são uma das ferramentas criptográficas mais avançadas na tentativa de equilibrar transparência e privacidade em blockchains. Seu princípio básico é a capacidade de comprovar a veracidade de uma informação sem divulgar seu conteúdo subjacente. Em termos técnicos, uma parte,

95 *Bootstrapping* é definido como “puxar-se para cima pelas próprias amarras”, segundo o Dicionário Oxford. “Quando dizemos que um esquema de criptografia homomórfica pode sofrer *bootstrapping*, significa que ele pode avaliar homomorficamente seu próprio procedimento de descriptografia”. Ver mais em: BADAWI, Al Ahmad; POLYAKOV, YURIY. *Demystifying Bootstrapping in Fully Homomorphic Encryption*. Duality Technologies, 2023. Disponível em: Link. Acesso em: 4 out. 2025.

96 GONG, Yanwei et al. *Practical Solutions in Fully Homomorphic Encryption: A Survey Analyzing Existing Acceleration Methods*. *Cybersecurity*, v. 7, n. 1, 2024. DOI: 10.1186/s42400-023-00187-4. Disponível em: Link. Acesso em: 4 out. 2025.

97 Ibid.

chamada provador, consegue comprovar, para a outra parte, chamada verificador, de que possui um certo conhecimento ou informação, sem revelá-lo. As ZKPs se assemelham aos *commitments schemes* tratados anteriormente, ambos mantêm o segredo oculto, mas as ZKPs são mais sofisticadas pois permitem provar a veracidade de uma afirmação sem nunca revelar o dado e sem exigir uma fase posterior de revelação. Inclusive, na prática, *commitments* são frequentemente usados como componentes dentro das ZKPs. Essa característica faz com que as ZKPs sejam particularmente importantes em situações em que a verificação de autenticidade deve ser realizada sem violar a privacidade dos dados pessoais⁹⁸.

Shafi Goldwasser, Silvio Micali e Charles Rackoff foram os primeiros a apresentar o conceito, em 1985, quando introduziram as provas interativas de conhecimento zero. Posteriormente, esse conceito evoluiu para versões não interativas (NIZK), aplicáveis aos sistemas descentralizados⁹⁹. Em blockchains, essas provas são frequentemente usadas para verificar a autenticidade de transações ou identidades sem expor informações sensíveis. Iniciativas como Zcash e zkSync ilustram a aplicação prática dessa metodologia, empregando variantes como zk-SNARKs (*Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge*) e zk-STARKs (*Zero-Knowledge Scalable Transparent Arguments of Knowledge*), que diminuem a necessidade por interação e melhoram a eficácia¹⁰⁰.

O valor jurídico e regulatório das ZKPs reside em sua capacidade de conciliar o princípio da transparência, fundamental para blockchains públicas, com o princípio da minimização de dados, estabelecido na LGPD e no GDPR. Ao permitir que a verificação de uma operação seja realizada sem revelar o conteúdo subjacente, essas provas diminuem

98 GOLDWASSER, Shafi; MICALI, Silvio; RACKOFF, Charles. *The Knowledge Complexity of Interactive Proof Systems*. *SIAM Journal on Computing*, v. 18, n. 1, p. 186–208, 1989. Disponível em: Link. Acesso em: 05 out. 2025.

99 Ibid.

100 BEN-SASSON, Eli et al. *Zerocash: Decentralized Anonymous Payments from Bitcoin*. In: *IEEE Symposium on Security and Privacy (SP 2014)*. Los Alamitos: IEEE, 2014. p. 1-53. Disponível em: Link. Acesso em: 05 out. 2025.

significativamente os riscos de reidentificação e cumprem o requisito de confidencialidade estabelecido no artigo 46 da LGPD¹⁰¹. Desse modo, elas podem ser consideradas implementações técnicas do conceito de *privacy by design*, uma vez que integram mecanismos de proteção de dados desde a concepção do sistema.

No espectro técnico-jurídico, as ZKPs permitem que os direitos individuais sejam exercidos sem comprometer a integridade dos registros. Por exemplo, um titular pode demonstrar que seus dados foram removidos ou anonimizados sem que a própria demonstração revele esses dados. Essa característica é especialmente valiosa em auditorias e verificações de conformidade, nas quais o controlador deve comprovar estar alinhado às normas de proteção de dados sem divulgar dados sensíveis. A literatura sugere que esse modelo pode ser utilizado como fundamento para “provas de conformidade criptográfica”, nos contextos em que a estrutura do código em si funciona como prova de conformidade normativa¹⁰².

No entanto, embora apresentem potencial, as provas de conhecimento zero ainda enfrentam dificuldades relacionadas à padronização, interoperabilidade e ao custo computacional. A geração e verificação de provas exigem um alto poder de processamento, o que restringe sua implementação em blockchains públicas de larga escala. Ademais, a falta de transparência é capaz de gerar conflitos regulatórios, pois auditorias ou *due diligences* jurídicas podem demandar algum grau de rastreabilidade¹⁰³. Assim, equilibrar a confidencialidade técnica com a transparência institucional continua sendo um dos principais obstáculos para a ampla adoção dessas *privacy-enhancing technologies*.

101 BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: Link. Acesso em: 6 out. 2025.

102 FINCK, Michèle. *Blockchain Regulation and Governance in Europe*. Cambridge: Cambridge University Press, 2019, p. 97-101. Disponível em: Link. Acesso em: 6 out. 2025.

103 EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY (ENISA). *Privacy-Enhancing Technologies (PETs): State of the Art and Future Directions*. Athens: ENISA, 2023. p. 44–46. Disponível em: Link. Acesso em: 06 out. 2025.

As ZKPs, em perspectiva, constituem um ponto de inflexão na convergência entre criptografia e governança. Além de manterem a integridade e autenticidade das informações, elas também transformam o conceito de confiança nas transações digitais, movendo-o do âmbito institucional para o matemático. Essa mudança sugere um modelo de conformidade descentralizada, em que as normas jurídicas e os princípios de proteção de dados são incorporados diretamente ao código.

9. PRUNING

A crescente expansão das blockchains públicas, resultado direto de sua estrutura imutável e distribuída, tem levado os pesquisadores a explorarem métodos que diminuam a quantidade de dados armazenados sem afetar a segurança e a verificabilidade da rede. Dentre as soluções sugeridas, o *pruning*, ou poda seletiva de dados, se sobressai como uma abordagem promissora para conciliar a necessidade de retenção de informações com as obrigações legais de exclusão e minimização estabelecidas em legislações como a LGPD e GDPR¹⁰⁴.

Tecnicamente, o *pruning* envolve a remoção controlada de blocos ou transações antigas que já foram incorporadas ao estado atual da rede, mantendo apenas os metadados necessários para assegurar a integridade da cadeia. Essa prática não infringe o princípio da imutabilidade, uma vez que os blocos originais continuam validados e registrados historicamente, mesmo que não sejam necessariamente armazenados em sua totalidade em cada nó. Portanto, o foco não está em apagar dados, mas em diminuir a redundância da informação distribuída. Isso permite que certos nós mantenham versões

104 ABDELHAMID, Mohamed Moetez et al. *ABISchain: Towards a Secure and Scalable Blockchain Using Swarm-based Pruning*. In: *Australian Computer Science Week (ACSW 2023)*. Melbourne: ACM, 2023. p. 1–8. DOI: 10.1145/3579375.3579420. Disponível em: Link. Acesso em: 06 out. 2025.

condensadas da blockchain, o que é suficiente para verificar transações válidas no futuro¹⁰⁵.

A literatura recente tem se dedicado a tornar esse processo mais eficaz e passível de verificação. No estudo *CoinPrune*, divulgado por Matzutt e outros, os autores apresentam um modelo de poda segura para blockchains públicas. Esse modelo possibilita a remoção de blocos antigos por meio da compressão de estados e reancoragem de hashes, mantendo a consistência global da rede. O método utiliza provas criptográficas de consistência e *merkle roots* resumidas, assegurando que blocos excluídos possam ser validados posteriormente sem a necessidade de manter o conteúdo completo da cadeia. Os resultados indicam uma redução significativa no tamanho do *ledger*, mantendo a auditabilidade e a verificabilidade, que são fundamentais para a segurança jurídica de registros distribuídos¹⁰⁶.

Adicionalmente, o estudo de Palm, Schelén e Bodin apresenta a noção de predicados de poda (*pruning predicates*), possibilitando que cada nó exclua transações redundantes ou que se cancelem mutuamente, sem comprometer a reconstrução do estado derivável da rede¹⁰⁷. Já Abdelhamid et al. desenvolveram o ABISchain, um modelo fundamentado na inteligência de enxame (*swarm-based pruning*). Nesse modelo, algoritmos de otimização distribuída escolhem de forma dinâmica as transações a serem eliminadas, preservando apenas os componentes essenciais para a consistência global. Em conjunto, essas pesquisas mostram que a redução seletiva e segura de dados

105 MATZUTT, Roman et al. *How to Securely Prune Bitcoin's Blockchain (CoinPrune)*. In: *IFIP Networking Conference 2020*. IFIP, 2020. p. 1–9. Disponível em: Link. Acesso em: 7 out. 2025.

106 MATZUTT, Roman et al. *How to Securely Prune Bitcoin's Blockchain (CoinPrune)*. In: *IFIP Networking Conference 2020*. IFIP, 2020. p. 5–7. Disponível em: Link. Acesso em: 7 out. 2025.

107 PALM, Emanuel; SCHELÉN, Olov; BODIN, Ulf. *Selective Blockchain Transaction Pruning and State Derivability*. In: *IEEE International Conference on Cyber Security and Blockchain (CVCBT 2018)*. Piscataway: IEEE, 2018. p. 1–10. DOI: 10.1109/CVCBT.2018.00009. Disponível em Link. Acesso em: 7 out. 2025.

pode estar alinhada com os princípios de integridade e auditabilidade da blockchain.¹⁰⁸

Sob a ótica da proteção de dados, o *pruning* pode funcionar como um método de exclusão funcional ou lógica, conceito já aceito por autoridades de privacidade, no qual a informação deixa de ser acessível e processável, mesmo que tecnicamente continue registrada de forma agregada ou criptografada¹⁰⁹. Dessa forma, a técnica surge como uma opção intermediária entre a exclusão física inviável e a imutabilidade absoluta, cumprindo os princípios de minimização, limitação de armazenamento e necessidade estabelecidos nas legislações de proteção de dados.

Não obstante, o uso de *pruning* também apresenta desafios. A eliminação seletiva de dados exige critérios claros e passíveis de verificação, sob pena de comprometer a integridade probatória da cadeia. Além disso, há o risco de que diferentes políticas de poda implementadas por *nodes* distintos possam levar à fragmentação de estados e inconsistências regulatórias. Portanto, a implementação dessa técnica em contextos de proteção de dados deve ser complementada de mecanismos de verificação criptográfica compartilhada, como *merkle proofs* e *state commitments*, os quais asseguram a autenticidade do histórico mesmo após a redução de dados armazenados.

Em síntese, o *pruning* não apenas contribui para a escalabilidade e sustentabilidade das redes blockchain, como também proporciona um meio prático de conciliação com as obrigações de eliminação e anonimização de dados pessoais. Essa abordagem confirma a viabilidade de um modelo de compliance criptográfico, no qual a segurança dos dados é garantida não só por meio de regulamentações, mas também pelo design intrínseco da infraestrutura tecnológica, ao minimizar o armazenamento de dados supérfluos e preservar apenas o essencial para a validação.

108 ABDELHAMID, Mohamed Moetez et al. Op. cit. p. 4-6. Disponível em: Link. Acesso em: 7 out. 2025.

109 AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). *Estudo Preliminar sobre Anonimização e Pseudonimização para a proteção de dados pessoais*. Brasília: ANPD, 2023. p. 10-11. Disponível em: Link. Acesso em: 7 out. 2025.

10. CHAMELEON HASHES

Alguns participantes desenvolveram blockchains “editáveis” utilizando funções de *chameleon hashes* para modificar, excluir ou reescrever certos dados¹¹⁰, como forma de preservar a privacidade e atender a exigências regulatórias¹¹¹. Os *chameleon hashes*, ou funções hash camaleônicas representam uma variação das funções hash tradicionais, permitindo a ocorrência de colisões controladas. Em uma função hash convencional, qualquer modificação no conteúdo original produz um resultado (ou *digest*) totalmente diferente, assegurando a imutabilidade e a integridade dos dados. Nas funções camaleônicas, existe um componente extra chamado *trapdoor key* (ou chave de armadilha), que possibilita a uma entidade autorizada gerar um novo valor de hash para uma mensagem alterada, mantendo o exato resultado da função.

Em termos práticos, trata-se de uma função hash com propriedades semelhantes às de um camaleão, o que justifica o nome do tipo de função e a característica de mutabilidade: somente quem possui a chave secreta pode gerar uma colisão válida. Dessa forma, é possível modificar o conteúdo subjacente sem quebrar a cadeia de blocos, preservando a validade criptográfica do registro. Essa propriedade faz com que os *chameleon hashes* sejam uma ferramenta potencial para implementar o direito de retificação ou eliminação de dados em sistemas baseados em blockchain, mantendo a auditabilidade global da rede intacta.

Como bem aponta Finck, dependendo do design específico dessas soluções, elas podem facilitar¹¹² a conformidade com o GDPR

110 Ver mais em: ZHAO, Yuqi et al. *A privacy-preserving and secure editable blockchain model for government data sharing*. In: *The Journal of Supercomputing*. Springer, 2025. Disponível em: Link. Acesso em: 8 out. 2025.

111 FINCK, Michèle. *Blockchain and the General Data Protection Regulation*. European Parliamentary Research Service (EPRS), 2019. p. 34. Disponível em: Link. Acesso em: 8 out. 2025.

112 FINCK, Michèle. *Blockchain and the General Data Protection Regulation*. European Parliamentary Research Service (EPRS), 2019. **Executive summary** (passagens

e a LGPD. No entanto, fica evidente que, uma vez que uma blockchain torne-se editável, o argumento inicial para o uso dessa solução em oposição a outras formas de bancos de dados (distribuídos) pode ser derrotado. Isso, no entanto, dependerá em parte dos arranjos de governança envolvidos.

11. EMBASAMENTO JURÍDICO E PERSPECTIVAS FUTURAS

A análise das soluções criptográficas propostas demonstra um esforço coletivo da comunidade científica e regulatória em conciliar a inovação tecnológica da blockchain com os fundamentos da proteção de dados pessoais. Contudo, o cenário normativo ainda possui lacunas consideráveis em relação à sua aplicabilidade, principalmente no que diz respeito à atribuição de responsabilidades, exercício dos direitos do titular e estabelecimento de mecanismos técnicos equivalentes à exclusão de dados.

Tanto o GDPR europeu quanto a LGPD brasileira foram desenvolvidos em um âmbito de tratamento de dados centralizado, com a presença de controladores claramente identificáveis, responsáveis pelas decisões relacionadas ao tratamento. Por outro lado, a blockchain pública e descentralizada funciona sem uma estrutura de controle hierárquica, distribuindo a gestão, o consenso e a validação de dados entre seus participantes. Essa natureza difusa desafia a lógica jurídica convencional, dificultando a identificação de quem seria, em última instância, o controlador ou operador dos dados para fins de conformidade¹¹³.

Nesse mesmo diapasão, as soluções criptográficas examinadas, como *hashes* e *commitments*, *crypto-shredding*, criptografia homomórfica, provas de conhecimento zero, *pruning* e *chameleon hashes* funcionam como ferramentas de conformidade regulatória da

iniciais). Disponível em: Link. Acesso em: 8 out. 2025.

113 FINCK, Michèle. *Blockchain and the General Data Protection Regulation*. European Parliamentary Research Service (EPRS), 2019. p. 27-29. Disponível em: Link. Acesso em: 8 out. 2025.

tecnologia, mesmo que não resolvam de forma definitiva o conflito entre imutabilidade e exclusão. Do ponto de vista jurídico, essas técnicas podem ser vistas como estratégias de “exclusão funcional” ou “anonimização reforçada”, alinhadas com a intenção dos legisladores apontada nos artigos 17 e 25 do GDPR e 18 e 46 da LGPD, que preveem o uso de soluções técnicas e organizacionais adequadas para assegurar a proteção de dados pessoais¹¹⁴.

No entanto, a implementação dessas medidas requer uma reinterpretação das normas e um diálogo regulatório contínuo entre juristas, engenheiros e autoridades de proteção de dados. O European Data Protection Board (EDPB) já reconheceu a necessidade de abordagens flexíveis que levem em conta a criptografia e a descentralização como mecanismos legítimos de conformidade. O EDPB sugere que a utilização de blockchain seja analisada com base nos princípios da proporcionalidade e da finalidade, e não somente sob o critério formal da exclusão absoluta.¹¹⁵ No Brasil, a ANPD adota uma abordagem similar, enfatizando que a pseudonimização e anonimização podem, em certos casos, atender aos requisitos de eliminação de dados, desde que sejam documentados em Relatórios de Impacto (RIPD) e acompanhados de boas práticas de governança¹¹⁶.

Em termos de viabilidade, as soluções técnicas ainda se deparam com desafios relacionados a custos e padronização, particularmente nas blockchains públicas, em que a imutabilidade dos registros é um requisito fundamental para o consenso (confiança) da rede. No entanto, nota-se um movimento de colaboração entre instituições acadêmicas,

114 BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: Link. Acesso em: 8 out. 2025. EUROPEAN UNION. *Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR)*. Official Journal of the European Union, 2016.

115 EUROPEAN DATA PROTECTION BOARD (EDPB). *Guidelines 02/2025 on the processing of personal data through blockchain technologies*. Bruxelas: EDPB, 2025. Disponível em Link. Acesso em: 8 out. 2025.

116 AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). *Estudo Preliminar sobre Anonimização e Pseudonimização para a proteção de dados pessoais*. Brasília: ANPD, 2023. p. 12-14. Disponível em: Link. Acesso em: 8 out. 2025.

setor privado e entidades reguladoras na criação de modelos híbridos e protocolos de governança que atendam às demandas legais. Espera-se que, a médio prazo, o direito avance na criação de uma regulação eficaz, que não se concentre apenas na eliminação formal de dados, mas também na garantia concreta dos direitos dos titulares por meios técnicos verificáveis.

Em suma, a harmonização entre blockchain e proteção de dados não deve ser considerada um paradoxo sem solução, mas sim um processo de convergência gradual entre a autonomia tecnológica e finalidade e segurança jurídica. As técnicas criptográficas analisadas aqui demonstram que a conformidade regulatória pode ser obtida não por meio da supressão da inovação, mas pela sua incorporação deliberada ao desenho normativo, com a colaboração da academia, da comunidade científica e dos reguladores nacionais e supranacionais. Este percurso que simboliza, simultaneamente, um desafio e uma oportunidade para o futuro da regulação digital.

12. CONSIDERAÇÕES FINAIS

A análise realizada neste estudo demonstrou que a relação entre a tecnologia blockchain e a proteção de dados pessoais requer soluções que integrem a segurança técnica ao atendimento das normativas de privacidade. No mesmo sentido, o conflito entre a imutabilidade dos registros e o direito à eliminação de dados, estabelecido na LGPD e no GDPR, não se trata de uma questão absoluta, mas sim de compatibilização prática e interpretativa.

As alternativas criptográficas analisadas, como funções hash, chaves rotativas, *crypto-shredding*, criptografia homomórfica, provas de conhecimento zero e *pruning*, demonstram que é possível implementar mecanismos que reduzam o risco de reidentificação e assegurem a inutilização funcional dos dados. Essas técnicas não eliminam integralmente o dado da cadeia, mas atendem ao princípio da minimização e permitem alcançar um grau razoável de conformidade sem comprometer a integridade do sistema distribuído.

Sob a perspectiva jurídica, verifica-se que o ordenamento ainda carece de parâmetros normativos claros para o tratamento descentralizado de dados. Entretanto, tanto a LGPD quanto o GDPR incentivam o uso de medidas técnicas apropriadas a assegurar a proteção de dados, possibilitando a inclusão de soluções criptográficas como ferramentas legítimas para conformidade regulatória.

Conclui-se, portanto, que a compatibilização entre blockchain e proteção de dados depende do desenvolvimento de uma regulação funcional, que reconheça o papel da criptografia na concretização dos princípios da privacidade e da segurança da informação, inclusive no campo jurídico. A evolução normativa e técnica deverá ocorrer de forma conjunta, de modo a permitir que os avanços tecnológicos sejam acompanhados por interpretações jurídicas coerentes com a realidade digital contemporânea.

13. REFERÊNCIAS

ABROL, Ayushi. Blockchain vs. Distributed Ledger Technology. *Blockchain Council*, 2018. Disponível em: <https://www.blockchain-council.org/blockchain/blockchain-vs-distributed-ledger-technology/>. Acesso em: 7 ago. 2025.

ARTICLE 29 WORKING PARTY. *Opinion 04/2007 on the concept of personal data (WP 136) 01248/07/EN*, 21. p. 17-20. Disponível em: <https://www.pdp.ie/docs/1030.pdf>. Acesso em: 14 out. 2025.

ARTICLE 29 WORKING PARTY. *Opinion 05/2012 on Cloud Computing (WP 196) 01037/12/EN*, 12. p. 20-21. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf. Acesso em: 14 out. 2025.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). *Estudo preliminar sobre anonimização e pseudonimização para a proteção de dados pessoais*. Brasília: ANPD, 2023. Disponível em: <https://www.gov.br/participamaisbrasil/blob/baixar/37060>. Acesso em: 14 out. 2025.

BARKER, Elaine. *Recommendation for Key Management – Part 1: General (NIST Special Publication 800-57, Rev. 5)*. Gaithersburg: National Institute of Standards and Technology, 2023. Disponível em: <https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final>. Acesso em: 14 out. 2025.

BEN-SASSON, Eli et al. *Zerocash: Decentralized Anonymous Payments from Bitcoin*. In: *IEEE Symposium on Security and Privacy (SP 2014)*. Los Alamitos: IEEE, 2014. p. 1-53. Disponível em: https://www.researchgate.net/publication/286668243_Zerocash_Decentralized_Anonymous_Payments_from_Bitcoin. Acesso em: 14 out. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago.

2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em: 14 out. 2025.

CASEY, Michael et al. *The Impact of Blockchain Technology on Finance: A Catalyst for Change*. Geneva: ICMB, 2018, p. 14. Disponível em: <https://www.cimb.ch/uploads/1/1/5/4/115414161/geneva21.pdf>. Acesso em: 14 out. 2025.

CASTOR, Amy. *Why Ethereum is switching to proof of stake and how it will work*. MIT Technology Review, 2022. Disponível em: <https://www.technologyreview.com/2022/03/04/1046636/ethereum-blockchain-proof-of-stake/>. Acesso em: 14 out. 2025.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

EUROPEAN DATA PROTECTION BOARD (EDPB). *Guidelines 02/2025 on the processing of personal data through blockchain technologies*. Bruxelas: EDPB, 2025. Disponível em: https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/guidelines-022025-processing-personal-data_en. Acesso em: 14 out. 2025.

EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY (ENISA). *Privacy-Enhancing Technologies (PETs): State of the Art and Future Directions*. Athens: ENISA, 2023. p. 44–46. Disponível em: <https://www.enisa.europa.eu/sites/default/files/publications/Readiness%20Analysis%20for%20the%20Adoption%20and%20Evolution%20of%20Privacy%20Enhancing%20Technologies.pdf>. Acesso em: 14 out. 2025.

FINCK, Michèle. *Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?* Bruxelas: European Parliamentary Research Service, 2019. Disponível em: <https://www.europarl.europa.eu/RegData/etudes/>

STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf. Acesso em: 14 out. 2025.

FINCK, Michèle. *Blockchain Regulation and Governance in Europe*. Cambridge: Cambridge University Press, 2019, p. 42. Disponível em: <https://www.cambridge.org/core/books/blockchain-regulation-and-governance-in-europe/A722E0522BC6C5300AA0813340BD6C04>. Acesso em: 14 out. 2025.

FINCK, Michèle; MOSCON, Valeria. *Copyright Law on Blockchains: Between New Forms of Rights Administration and Digital Rights Management 2.0*. JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law, v. 10, n. 1, 2019. Disponível em: https://www.researchgate.net/publication/329820077_Copyright_Law_on_Blockchains_Between_New_Forms_of_Rights_Administration_and_Digital_Rights_Management_20. Acesso em: 14 out. 2025.

GENTRY, Craig. *A Fully Homomorphic Encryption Scheme*. Stanford University, 2009. (Tese de Doutorado). Disponível em: <https://crypto.stanford.edu/craig/craig-thesis.pdf>. Acesso em: 14 out. 2025.

GOLDWASSER, Shafi; MICALI, Silvio; RACKOFF, Charles. *The Knowledge Complexity of Interactive Proof Systems*. SIAM Journal on Computing, v. 18, n. 1, p. 186–208, 1989. Disponível em: https://people.csail.mit.edu/silvio/Selected%20Scientific%20Papers/Proof%20Systems/The_Knowledge_Complexity_Of_Interactive_Proof_Systems.pdf. Acesso em: 14 out. 2025.

GONG, Yanwei et al. *Practical Solutions in Fully Homomorphic Encryption: A Survey Analyzing Existing Acceleration Methods*. Cybersecurity, v. 7, n. 1, 2024. DOI: 10.1186/s42400-023-00187-4. Disponível em: <https://cybersecurity.springeropen.com/articles/10.1186/s42400-023-00187-4>. Acesso em: 14 out. 2025.

LIN, Iuon-Chang; LIAO, Tzu-Chun. A Survey of Blockchain Security Issues and Challenges. *International Journal of Network Security*, v. 19, n. 5, p. 653–659, 2017. Disponível em: <http://ijns.jalaxy.com.tw/contents/ijns-v19-n5/ijns-2017-v19-n5-p653-659.pdf>. Acesso em: 14 out. 2025.

NAKAMOTO, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 14 out. 2025.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). *Special Publication 800-88 Revision 1: Guidelines for Media Sanitization*. Gaithersburg, 2014. p. 13-15. Disponível em: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf>. Acesso em: 14 out. 2025.

PACE, Emma; DE FILIPPI, Primavera. *Blockchain and Privacy: Towards a Technical and Legal Reconciliation*. *Computer Law & Security Review*, v. 44, 2022.

PAILLIER, Pascal. *Public-Key Cryptosystems Based on Composite Degree Residuosity Classes*. In: *Advances in Cryptology – EUROCRYPT '99*. Berlin: Springer, 1999. p. 223–238. Disponível em: https://www.researchgate.net/publication/221348062_Public-Key_Cryptosystems_Based_on_Composite_Degree_Residuosity_Classes. Acesso em: 14 out. 2025.

PEDERSEN, Torben. *Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing*. In: *Advances in Cryptology – CRYPTO '91*. Springer, 1992. p. 129–140. Disponível em: https://reaction.la/security/pedersons_secret_sharing.pdf. Acesso em: 14 out. 2025.

SCHREIBER, Anderson. *Tratado de Direito Civil: responsabilidade civil*. São Paulo: Atlas, 2020.

SCHWARTZ, Paul; SOLOVE, Daniel. *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*. *Harvard Law Review*, v.

86, 2011, p. 1814–1892. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1909366. Acesso em: 27 set. 2025.

SOLOVE, Daniel J. *Understanding Privacy*. Cambridge: Harvard University Press, 2008, p. 117. Disponível em: <https://www.hup.harvard.edu/books/9780674035072>. Acesso em: 14 out. 2025.

STALLINGS, William. *Cryptography and Network Security: Principles and Practice*. 5. ed. New York: Pearson, 2010. p. 329–353. Disponível em: https://www.uoitc.edu.iq/images/documents/informatics-institute/Competitive_exam/Cryptography_and_Network_Security.pdf. Acesso em: 14 out. 2025

TAPSCOTT, Don; TAPSCOTT, Alex. *Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World*. New York: Penguin, 2016.

TAPSCOTT, Don; TAPSCOTT, Alex. *Realizing the Potential of Blockchain*. World Economic Forum, 2017, p. 5. Disponível em: https://www3.weforum.org/docs/WEF_Realizing_Potential_Blockchain.pdf. Acesso em: 7 ago. 2025.

VOIGT, Paul; VON DEM BUSSCHE, Axel. *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Cham: Springer, 2024, p. 202. Disponível em: <https://link.springer.com/book/10.1007/978-3-031-62328-8>. Acesso em: 14 out. 2025.

ZHAO, Yuqi et al. *A privacy-preserving and secure editable blockchain model for government data sharing*. In: *The Journal of Supercomputing*. Springer, 2025. Disponível em: <https://link.springer.com/article/10.1007/s11227-025-07388-3>. Acesso em: 8 out. 2025

4. BLOCKCHAIN COMO INVESTIMENTO ESTRATÉGICO PARA AVERIGUAÇÃO DA SUSTENTABILIDADE NA CADEIA DE SUPRIMENTOS

Karina Chagas dos Santos

Especialista em Direito Digital pelo Instituto de Tecnologia e Sociedade do Rio de Janeiro – ITS Rio em parceria com o Centro de Estudos e Pesquisas no Ensino do Direito da Universidade do Estado do Rio de Janeiro (CEPED/ UERJ).

INTRODUÇÃO

A Blockchain é uma invenção tecnológica recente que permite, através de uma sequência contínua de blocos, o registro de todas as transações de forma descentralizada, garantindo maior segurança, transparência e confiabilidade nos dados, uma vez que são imutáveis.

Inicialmente, o algoritmo foi criado junto ao ramo financeiro, como um livro razão, descentralizado, que torna transparente todas as transações realizadas através do armazenamento dos dados, tornando acessível as suas informações e, por consequência, tornando transparente e segura as transações financeiras com a criptografia.

Com a blockchain, o processo de rastreabilidade das movimentações, inicialmente, ligadas às criptomoedas, concedia maior confiabilidade e segurança na rastreabilidade das movimentações financeiras, já que com a tecnologia, a informação chega a todos os envolvidos, sem a necessidade de uma terceira pessoa para validá-la.

Assim, diante da sua confiabilidade e com o estudo dos seus impactos positivos, a tecnologia se expandiu para tornar eficaz outros tipos de movimentações, como, por exemplo, sua aplicação na rastreabilidade da cadeia de suprimentos.

Nesse tipo de situação, a cadeia de suprimentos utiliza a blockchain no intuito de deixar evidente todas as movimentações que ocorrem até a distribuição do produto a ser consumido, o que

torna transparente a movimentação ocorrida e, consequentemente, ajudando a torná-la uma cadeia sustentável.

O seu uso beneficia o desenvolvimento sustentável da empresa, uma vez que melhora o gerenciamento da cadeia de suprimentos, possibilitando o rastreamento todo o processo produtivo daquele bem e/ou serviço, desde a gestão desses produtos até a rastreabilidade das preferências de compra do consumidor. (Santos et.al, 2024)

1. BLOCKCHAIN: FUNDAMENTOS E APLICAÇÕES

A tecnologia blockchain, atualmente, pode ser considerada uma das tecnologias mais úteis e revolucionárias do mundo digital.

Por ser considerada uma forma segura de gerenciamento de dados, a blockchain, inicialmente inserido no contexto financeiro, - com a criação das criptomoedas -, funciona de forma segura e transparente, especialmente para controle de informações ligadas às transações financeiras. (Montezino, 2023)

A sua praticidade e segurança é atrativa pois a tecnologia blockchain funciona como um livro-razão, através de blocos que possuem criptografia, para registro de todas as transações, como uma “impressão digital”, que é imutável.

Como Montezino (2023) bem define:

A blockchain é uma tecnologia de registro de dados que permite a criação de um registro compartilhado e imutável de informações. Ela foi originalmente desenvolvida para ser usada na criptomoeda Bitcoin, mas tem sido utilizada para uma variedade de outras aplicações. Ao invés de armazenar os dados em um único lugar, como um banco de dados centralizado, a informação é armazenada em vários computadores em uma rede. Cada computador na rede possui uma cópia da cadeia de blocos, que é uma série de blocos de dados criptografados e interligados. Cada novo bloco adicionado à cadeia contém uma quantidade de transações e uma referência ao bloco anterior. Isso significa que, uma vez que um bloco é adicionado à cadeia, ele é muito difícil de ser alterado ou excluído.

Além da sua característica de imutabilidade, a blockchain também assegura a rastreabilidade e integralidade das informações.

Seu criador, Nakamoto, identifica no site oficial da bitcoin (2025) a tecnologia blockchain como bloco compartilhado publicamente com habilidade de rastrear e assegurar, através da criptografia, todas as transações e seus proprietários, mantendo assim a integralidade da transação:

A blockchain é um livro de registro de contabilidade público compartilhado no qual toda a rede Bitcoin confia. Todas as transações confirmadas são incluídas na cadeia de blocos. Desta forma, as carteiras de Bitcoin podem calcular seu saldo disponível e novas transações podem ser verificadas para que se possa usar bitcoins que são realmente de propriedade de quem está gastando. A integridade e ordem cronológica da cadeia de blocos são protegidas por criptografia. (Bitcoin.org; 2025)¹¹⁷

A tecnologia, como dito, contribui para rastrear cada passo enfrentado relacionado àquela transação, de modo à assegurar que nada será modificado, já que o processo de transacionar se torna público, imutável e descentralizado, sem que haja possibilidade de sofrer riscos de fraudes e adulterações. (Beck et.al, 2017).

Em relação a descentralização do processo envolvido na aplicação da blockchain, a tecnologia é vista como inovadora, pois é capaz de alterar todo o sistema econômico e social do mundo, já que não mais será necessário haver um órgão centralizado controlador de toda informação.

Montezino (2023) defende que a descentralização é ponto-chave no sistema blockchain, pois torna toda a transação imune à ataques cibernéticos, dentro outras coisas:

A descentralização é conceito-chave por trás do Bitcoin e das criptomoedas em geral. Em um sistema descentralizado, não há

117 “The block chain is a shared public ledger on which the entire Bitcoin network relies. All confirmed transactions are included in the block chain. It allows Bitcoin wallets to calculate their spendable balance so that new transactions can be verified thereby ensuring they’re actually owned by the spender. The integrity and the chronological order of the block chain are enforced with cryptography”.

um único ponto de falha ou uma única entidade responsável pela manutenção e funcionamento do sistema. No caso do Bitcoin, isso é alcançado através da utilização de uma rede P2P, onde todos os nós da rede são igualmente importantes e contribuem para validação e registro das transações. A descentralização tem várias vantagens, como resistência a ataques cibernéticos, a incapacidade de uma entidade centralizada de controlar e manipular o sistema, e a resistência a falhas de sistema. A descentralização também permite a criação de sistemas financeiros alternativos, como o Bitcoin, que podem competir com os sistemas financeiros tradicionais e oferecer soluções mais seguras e eficientes para transações financeiras.

Para Beck (2017), a centralização nas mãos de uma entidade é vulnerável, pois está apta a erros eventuais ou até intencionais:

The global economic system depends on that individuals and organizations trust other entities to create, store, and distribute essential records. For example, banks construct and maintain the financial records, hospitals construct and maintain health records, and universities construct and maintain education records. Often, records central to our health, social, or professional lives are key records either constructed or maintained by third parties. Such third-party record repositories can be vulnerable to corruption by failure in storage systems or human mischief, which could be mitigated by unbiased and incorruptible blockchain-based digital systems (Beck et.al, 2017)¹¹⁸

Com o potencial que pode ser extraído da blockchain, qualquer forma de transação pode ser confiável, pois poderá ser segura

118 O sistema econômico global depende que os indivíduos e as organizações confiem em outras entidades para criar, armazenar e distribuir registros essenciais. Por exemplo, os bancos constroem e mantem os registros financeiros; hospitais constroem e mantem registros de saúde e universidades constroem e mantem registros educacionais. Frequentemente, os registros centrais da nossa saúde, da nossa vida social e profissional são registros chaves que são construídos e mantidos por terceiros. Tais repositórios de registros por terceiros pode ser vulneráveis à corrupção por falha de armazenamento ou por maldade humana, o que poderia ser mitigado por um sistema digital imparcial e incorrupto por blockchain.

contra fraude e inteiramente rastreável, dando total segurança e transparência.

A falta de um poder centralizado controlando as informações de uma transação já é um benefício de alto potencial extraído da blockchain. Para Beck et.al (2017):

In other words, it could provide a decentralized global information infrastructure in which no one is in full control, no one has absolute power, and no one can distort or lie about past or current events. (Beck et.al, 2017)¹¹⁹

A promessa de uma tecnologia capaz de facilitar e potencializar a confiabilidade de transações não só financeiras, torna fácil a sua aderência em outros campos, pois, apesar de primeiramente ter sido inventada com o intuito de ser aplicada às questões financeiras, hoje se estuda a possibilidade de utilização da blockchain em outras áreas, como, por exemplo, na cadeia de suprimentos e, ainda, para garantir direitos autorais.

2. SUSTENTABILIDADE NA CADEIA DE SUPRIMENTOS

A crescente preocupação mundial com os impactos negativos gerados pelas atividades empresariais no que tange às questões ambientais, sociais e econômicas, gera uma necessidade coletiva de repensar as práticas de gestão definidas por entidades empresariais.

Os impactos negativos causados pelas práticas empresariais nos levou à obrigatoriedade de alcançarmos uma responsabilidade corporativa, na qual a empresa deve atender às exigências legais e, além disso, se comprometer a integrar às suas atividades, práticas sustentáveis para assegurar atividades corporativas ambientalmente corretas, socialmente justas e economicamente viáveis.

Com isso, a Organização das Nações Unidas (ONU), organização intergovernamental que busca a promoção da paz e a segurança,

¹¹⁹ Em outras palavras, a blockchain pode providenciar uma infraestrutura informacional global descentralizada em que ninguém está em controle total e não há poder absoluto, sem poder distorcer ou mentir sobre eventos passados e atuais.

estabeleceu objetivos de desenvolvimento sustentável (ODS) em que se estipulam algumas metas globais a serem atingidas por países-membros, sociedade e empresas, com o objetivo de alcançar metas de erradicação da pobreza; segurança alimentar e agricultura; saúde; educação; igualdade de gênero; redução das desigualdades; energia; água e saneamento; padrões sustentáveis de produção e de consumo; proteção e uso sustentável dos oceanos e ecossistemas terrestres; crescimento econômico inclusivo; infraestrutura e industrialização; governança, meios de implementação e mudanças do clima. (Ministério do Meio Ambiente e Mudança do Clima, 2022)

Dentro desse parâmetro, a abordagem sustentável não só deve ser alcançada por entidades governamentais, como também pela sociedade e pelas empresas.

As empresas cada vez mais identificam que adotar práticas sustentáveis em prol da preservação do meio ambiente, ética nas relações sociais e mitigação dos riscos operacionais também lhes dão vantagens econômicas.

Para tanto, a gestão da sustentabilidade na cadeia de suprimentos emerge como elemento essencial para empresas atingirem as metas de sustentabilidade definidas pelas ODS, com o intuito de mitigar riscos e viabilizar as práticas ambientais, sociais e econômicas de forma sustentável.

A gestão de sustentabilidade da cadeia de suprimentos servirá para integrar todas as fases dentro da cadeia de suprimentos, desde à busca de matérias-primas, até a sua chegada ao consumidor final, de forma a ajustar todas as etapas às práticas sustentáveis. (Lec, 2024)

Uma das formas de atingir metas de *Environmental, Social and Governance* (ESG) na cadeia de suprimentos é através da aplicação da *Triple Bottom Line* (TBL), método utilizado para dimensionar o seu desempenho financeiro e valorar as práticas sustentáveis ambientais e sociais, através da diminuição de desperdícios e melhorias na utilização de energia renovável.

Sob TBL, as empresas devem equilibrar os objetivos financeiros, ambientais e sociais. Isso pode incluir minimizar o desperdício,

melhorar a eficiência energética e usar energia renovável. Além disso, você deve envolver consumidores, fornecedores e funcionários para promover a sustentabilidade e a responsabilidade social. (Veritas, 2025)

Para alcance de uma cadeia de suprimentos sustentável é necessária a participação de todos os agentes que fazem parte dela com o intuito de tornar a cadeia de suprimentos ecológica, transparente e circular.

Nesse contexto, a determinação em se alcançar a sustentabilidade na cadeia de suprimentos é tanta, que o Pacto Global das Nações Unidas emitiu um guia prático com dez critérios para medição da sustentabilidade na cadeia de suprimentos de forma a contemplar as quatro áreas de interesse que se perfazem na promoção dos direitos humanos, melhorias nas condições de trabalho, proteção ao meio ambiente e combate à corrupção. (Sisco et.al, 2010)

Um dos objetivos do guia criado pelo Pacto Global das Nações Unidas é, para além de benefícios próprios para as empresas, orientá-las a alcançar metas de desenvolvimento sustentável na cadeia de suprimentos:

Hoje, os participantes do Compacto Global das Nações Unidas em todo o mundo estão demonstrando liderança pela aplicação de 10 princípios em suas cadeias de fornecimento. Entretanto, desenvolver programas de uma Cadeia de Suprimentos sustentável que abranjam todas as quatro áreas de interesse – direitos humanos, trabalho, meio ambiente e combate à corrupção – continua sendo um desafio desencorajador para muitos. Sustentabilidade da Cadeia de Suprimentos: Um Guia Prático para Aprimoramento Contínuo, desenvolvido em colaboração com o BSR, pode ajudar as empresas a superarem esses desafios oferecendo orientação prática sobre a forma de desenvolver um programa de cadeia de desenvolvimento sustentável com base nos valores e princípios do Compacto Global. Apresentando inúmeros exemplos de boas práticas corporativas, o guia assistirá as empresas a estabelecer prioridades por ação que conduza a um contínuo aperfeiçoamento de desempenho.

Um dos fatores em ascensão ao alcance das empresas, para minimizar danos em todo o processo na cadeia de suprimentos, é a utilização de soluções tecnológicas para controle da cadeia de suprimentos.

No próximo tópico desse estudo avaliaremos a blockchain como exemplo de solução tecnológica para ser aplicada na rastreabilidade da sustentabilidade na cadeia de suprimentos.

3. UTILIZAÇÃO DA BLOCKCHAIN PARA AVERIGUAÇÃO DA SUSTENTABILIDADE NA CADEIA DE SUPRIMENTOS

A sustentabilidade na cadeia de suprimentos predetermina a integração de todo o processo produtivo implementado desde a extração de recurso até a sua chegada ao consumidor, de forma a tornar essa cadeia mais confiável.

Ainda no contexto da cadeia de suprimentos sustentável, um dos focos principais para aumentar a confiabilidade de todo o processo da cadeia é o envolvimento de todos os seus participantes, ligado à possibilidade de averiguação e transparência de todas as atividades praticadas em relação àquele produto e serviço.

A adoção da tecnologia blockchain pode ser uma aliada benéfica para dar visibilidade a esse processo, como um meio inovador de rastreabilidade e transparência de toda a cadeia de suprimentos. (Santos et.al, 2024)

Em um estudo realizado pela Confederação Nacional da Indústria (CNI), (2021), foram apontados os benefícios de utilização da blockchain no comércio exterior. O Serviço Brasileiro de Apoio às Micro e Pequenas Empresas (SEBRAE), juntamente a CNI, desenvolveram o referido estudo para identificar os pontos positivos da aplicação da blockchain como ferramenta de gestão operacional do comércio brasileiro frente ao que já é aplicado globalmente. Identificou-se que, dentre os benefícios da tecnologia na aplicação no comércio exterior, estão:

A adoção da tecnologia blockchain já está se tornando um padrão na sistemática global do comércio exterior, motivo pelo qual a orientação do setor produtivo brasileiro, com vistas a adoção desta modalidade, é imprescindível. Trata-se de garantir a competitividade das empresas nacionais, expostas aos concorrentes do comércio exterior que aceleram suas adequações para operarem em um cenário de controle aduaneiro global totalmente digitalizado e integrado. O presente estudo procurou apresentar este cenário de transição e o potencial da tecnologia blockchain como ferramenta de gestão e eficiência operacional, mas, sobretudo, como estratégia de competitividade, a qual já venceu a barreira de tendência e passa a figurar como evolução tecnológica natural e irreversível para todas as cadeias produtivas e de valor do comércio exterior. Os motivos centrais estão evidenciados ao longo do estudo, com destaque para:

- Redução do tempo de trânsito (transit time) das cargas;
- Redução significativa da burocracia, otimizando custos com recursos humanos, agentes intermediários e recursos materiais;
- Padronização da operacionalidade das certificações internacionais;
- Atendimento às exigências cada vez mais rígidas das normativas globais relativas à segurança alimentar, pela via do rastreamento completo dos produtos desde a fonte da matéria prima até o ponto de venda e/ou retirada pelos consumidores;
- Facilitação dos processos de inspeção de produtos e auditoria documental;
- Modernização das aduanas, órgãos anuentes e órgãos fiscalizadores;
- Proteção de dados proporcionado pela computação distribuída, reduzindo as incidências de ataques cibernéticos;
- Contribuição com as normas internacionais de combate ao terrorismo e ataques biológicos em virtude da estrutura processual e sua transparência;
- Potencial de conversibilidade das criptomoedas como meios circulantes de pagamentos;
- Aceleração dos acordos e tratados internacionais de comércio, sejam bilaterais ou multilaterais;
- Crescimento exponencial das trocas comerciais pela via das plataformas globais de comércio eletrônico, com impacto na logística internacional;
- Mudanças no sistema financeiro internacional, com o advento das moedas digitais oficiais (yuan digital, dólar digital, euro

digital etc) facilmente integráveis à rede blockchain. (Confederação Nacional da Indústria, 2021)

A referida tecnologia é capaz de interligar todas as etapas e atores envolvidos na cadeia de suprimentos, como uma forma de governança das atividades realizadas, desde o fornecedor da matéria-prima, até a sua chegada ao consumidor final, sendo, portanto, útil em diversos processos na cadeia de suprimentos, permitindo a rastreabilidade do começo ao fim de toda a atividade envolvendo o produto em si, a extração do material utilizado, todas as transações pertencentes à essa cadeia, de modo a dar à todos os participantes a possibilidade de confirmar que todo o processo envolvido é sustentável e ético. (Santos et.al, 2024)

Para Pandey et.al (2023):

BT can be applied in a variety of processes to improve the Sustainability and resilience of the supply chain (Figure 1). For instance, allowing end-to-end traceability of products, materials, and transactions enables all supply chain participants to confirm the products' origin, authenticity, and quality. In order to confirm that a product was made sustainably and ethically, its path from raw materials to final delivery can be traced. Utilizing smart contracts can decrease the need for intermediaries and improve supply chain effectiveness. In addition, the transparent and unchangeable record of all transactions facilitates the identification of supply chain inefficiencies and possible bottlenecks, as well as can help cut down on waste and better resource allocation. BT can also be used to monitor a product's carbon impact throughout the entire supply chain. This makes it possible for businesses to find ways to lower their carbon emissions and carbon footprint and to take part in initiatives that reduce carbon emissions.¹²⁰

120 A tecnologia blockchain (BT) pode ser aplicada em diversos processos para melhorar a sustentabilidade e a resiliência da cadeia de suprimentos (Figura 1). Por exemplo, permitir a rastreabilidade de ponta a ponta de produtos, materiais e transações possibilita que todos os participantes da cadeia de suprimentos confirmem a origem, autenticidade e qualidade dos produtos. Para confirmar que um produto foi produzido de forma sustentável e ética, é possível rastrear seu percurso desde as matérias-primas até a entrega final. A utilização de smart contracts pode reduzir a necessidade de intermediários e aumentar a eficácia da cadeia de suprimentos. Além

Além disso, a blockchain também pode ser considerada uma aliada para combater possíveis falhas e seus riscos, pois aumenta a possibilidade de auditoria de/e por todas as pontas de conexão da cadeia.

O pesquisador Tiscini et. al (2020) identifica - em um estudo feito sobre a tecnologia blockchain como inovação para um modelo sustentável de negócios-, que especificamente quando se trata da indústria agroalimentar, a blockchain garante a segurança e rastreabilidade de maneira a assegurar a qualidade da cadeia de suprimentos, já que permite que o consumidor tenha acesso ao histórico do alimento, desde a produção até a distribuição, de modo que todo o processamento, desde a verificação do consumo de água, pode ser verificado pelo consumidor.

Para Tiscini et. al (2020), nos dias de hoje, os dados são a fonte de todas as transações. Com a referida tecnologia, qualquer transação, modificação ou atividade é comunicada através dos dados. Assim, lidar com grande número de dados, a todo tempo, requer assertividade e segurança que, hoje em dia, podem ser garantidos pela Blockchain:

Nowadays, data is considered to be the main value of Every transaction because each kind of physical operation, service providing or communication entails a data transfer. Dealing with big data requires assurance on quality and availability of information. To be useful to stakeholders, data-driven decisions require transparency, accountability and verifiability, and data has to be assured, verifiable and tamper-proof. Blockchain (BC) technology, mostly used and studied in financial transactions and applications (Nakamoto, 2008), has the features to meet all those requirements also in physical

disso, o registro transparente e imutável de todas as transações facilita a identificação de ineficiências e possíveis gargalos na cadeia, além de ajudar a reduzir desperdícios e melhorar a alocação de recursos. A BT também pode ser utilizada para monitorar o impacto de carbono de um produto ao longo de toda a cadeia de suprimentos. Isso permite que as empresas encontrem maneiras de reduzir suas emissões de carbono e participem de iniciativas de mitigação de emissões.

and service providing markets(Wang et al., 2019), like the agri-food industry¹²¹.

Além disso, a blockchain garante não só o controle de todos os dados através de uma tecnologia, mas permite que toda a transação que envolva qualquer dos participantes da cadeia seja sinérgico e integralizado, de modo coordenado e colaborativo, já que o mapeamento de toda a cadeia de suprimentos viabiliza a circulação das informações, contribuindo para a eficácia na gestão da cadeia de suprimentos sustentável por cada um dos agentes. (Aquino et.al, 2019)

Assim, são inúmeros os benefícios encontrados na utilização da blockchain na cadeia de suprimentos de forma a torná-la sustentável. No entanto, apesar de inúmeros benefícios de transparência na cadeia de suprimentos, a tecnologia ainda possui alguns desafios a serem enfrentados, que, para além da falta de regulamentação consolidada, também enfrenta desafios com os custos de investimentos, como a implementação da tecnologia e os custos de especialização para capacitação técnica, o que torna ainda mais difícil a sua utilização por pequenas e médias empresas e facilita a utilização da tecnologia por grandes empresas. (Gomes et.al, 2025)

Neste cenário, há algumas das grandes empresas que já começaram a utilizar a tecnologia blockchain como solução para rastreabilidade da sustentabilidade na cadeia de suprimentos.

A Walmart – multinacional estadunidense de loja de varejo –, em parceria com o *International Business Machines Corporation* (IBM) – empresa multinacional de tecnologia-, implementaram a blockchain na cadeia de suprimentos para melhora no controle da segurança

121 Atualmente, os dados são considerados o principal valor de cada transação, pois todo tipo de operação física, prestação de serviço ou comunicação envolve uma transferência de dados. Lidar com big data requer garantias quanto à qualidade e disponibilidade das informações. Para serem úteis aos stakeholders, as decisões baseadas em dados exigem transparência, responsabilidade e verificabilidade, e os dados precisam ser confiáveis, verificáveis e à prova de alterações. A tecnologia blockchain (BC), majoritariamente utilizada e estudada em transações financeiras e aplicações (Nakamoto, 2008), possui características que permitem atender a todos esses requisitos também em mercados de produtos físicos e prestação de serviços (Wang et al., 2019), como na indústria agroalimentar.

alimentar, através da rastreabilidade, pela tecnologia blockchain – *Hyperledger Fabric*-, da origem de mais de 25 produtos de 5 fornecedores diferentes (Walmart, 2018)

Outras grandes empresas, como Nestlé e Carrefour também passaram a utilizar a referida tecnologia para transparência ao consumidor na cadeia de suprimentos, de modo a garantir a sustentabilidade de todo o processo.

Assim, são inúmeros os benefícios encontrados na utilização da blockchain na cadeia de suprimentos de forma a torná-la sustentável.

CONSIDERAÇÕES FINAIS

Em síntese, a presente pesquisa demonstrou que há grandes benefícios na utilização da tecnologia blockchain de modo a assegurar a sustentabilidade na cadeia de suprimentos.

As práticas empresariais para alcance da cadeia de suprimentos sustentável se tornou foco importante que traz benefícios não só a sociedade como à própria empresa, já que há uma eficiência econômica ligada às práticas sustentáveis de redução de impactos negativos ambientais e sociais, que são pilares essenciais alinhados pela ONU com a definição dos ODS.

A tecnologia blockchain, nesse cenário, emerge como solução tecnológica para garantir a transparência e rastreabilidade da cadeia de suprimentos, de modo a aprimorar a governança de todo o processo da cadeia. A utilização estratégica da blockchain na cadeia de suprimentos, possibilita a transparência de todo o processo, de modo a garantir credibilidade das informações a todos os atores participantes e garantir que os riscos socioambientais sejam mitigados, melhorando assim o monitoramento das práticas sustentáveis da cadeia de suprimentos de diversos setores industriais.

Contudo, apesar dos inúmeros benefícios trazidos pela sua utilização, a implementação efetiva da tecnologia blockchain na cadeia de suprimentos ainda pode ser um desafio, levando em conta

o alto custo inicial para pôr em prática; limitações regulatórias e a necessidade de capacitação técnica dos agentes envolvidos.

O futuro, no entanto, aponta que há uma necessidade de investir em soluções inovadoras tecnológicas às gestões empresariais. Assim, conclui-se que a tecnologia blockchain representa uma ferramenta de grande potencial para impulsionar cadeias de suprimentos mais éticas, transparentes e sustentáveis.

REFERÊNCIAS

AQUINO, Magali. Adoção de blockchain na gestão de cadeias de suprimentos do Brasil. 2019. 86 f. Dissertação (Mestrado Profissional em Gestão para a Competitividade) – Escola de Administração de Empresas de São Paulo, Fundação Getulio Vargas, São Paulo, 2019. Disponível em: <https://repositorio.fgv.br/server/api/core/bitstreams/45f9aa0f-affb-476a-9745-2976467534e6/content>. Acesso em: 14 set. 2025.

BECK, Roman; AVITAL, Michel; ROSSI, Matti; TATCHER, Jason Bennett. Blockchain Technology in Business and Information Systems Research. *Bus Inf Syst Eng* 59, 2017. Disponível em: <https://doi.org/10.1007/s12599-017-0505-1>. Acesso em: 20 jul. 2025.

BITCOIN.ORG. Bitcoin.org: a comunidade do Bitcoin. Disponível em: <https://bitcoin.org/en/how-it-works>. Acesso em: 10 ago. 2025.

CONFEDERAÇÃO NACIONAL DA INDÚSTRIA. A tecnologia blockchain e suas possíveis aplicações no comércio exterior / Confederação Nacional da Indústria. – Brasília : CNI, 2021. 74 p. : il.

GOMES, Roberta Lima; VILLAÇA, Rodolfo da Silva; ALOCHIO, Gustavo Santa Clara; GOMES, Leonardo Lima; PEREIRA, Gesiane Silveira. Adoção de tecnologias blockchain na rastreabilidade em cadeias de suprimentos brasileiras. *P2P & Inovação – Informação e Plataformas Digitais*, Rio de Janeiro, v. 11, n. 2, p. 1-22, jan./jun. 2025. DOI: 10.21728/p2p.2025v11n2e-7318. Disponível em: <https://revista.ibict.br/p2p/article/view/7318/7163>. Acesso em: 20 nov. 2025.

LEC. O desafio da sustentabilidade: como integrar riscos e ODS. Disponível em: <https://lec.com.br/o-desafio-da-sustentabilidade-como-integrar-riscos-e-ods/#:~:text=Gest%C3%A3o%20da%20cadeia%20de%20suprimentos%3A%20C3%89%20essencial%20>

para,pr%C3%A1ticas%20ambientais%2C%20sociais%20e%20de%20governan%C3%A7a%20dos%20fornecedores. Acesso em: 10 ago. 2025.

MINISTÉRIO DO MEIO AMBIENTE e MUDANÇA DO CLIMA (MMA). Histórico dos ODS no MMA. Disponível em: <https://www.gov.br/mma/pt-br/acesso-a-informacao/informacoes-ambientais/historico-dos-ods-no-mma>. Acesso em: 10 ago. 2025.

MONTEZINO, Richard. Blockchain: da teoria à prática: tudo o que você precisa saber sobre a tecnologia que está revolucionando o mundo. São Paulo: Literare Books International, 2023.

PANDEY, Ajay Kumar; DAULTANI, Yash; PRATAP, Saurabh. Blockchain technology enabled critical success factors for supply chain resilience and sustainability. *Business Strategy and the Environment*, v. 33, n. 2, p. 1533–1554, 2024. DOI: 10.1002/bse.3548.

SANTOS, Paulo Henrique dos; CRUZ, José Elenilson; SOUZA, Daniel Soares de; LOPES, Cassiomar Rodrigues. Blockchain applied to sustainability in supply chains: proposing research agendas. *Revista RISUS (Journal on Innovation and Sustainability)*, v. 15, n. 1, p. 91-106, 29 abr. 2024. Disponível em: <https://revistas.pucsp.br/index.php/risus/article/view/65175>. Acesso em: 07 set. 2025.

SISCO, Cody; CHORN, Blythe; PRUZAN-JORGENSEN, Peder Michael et al. Sustentabilidade da Cadeia de Suprimentos: um Guia Prático para Aprimoramento Contínuo. 2010. Disponível em: https://d306pr3pise04h.cloudfront.net/docs/issues_doc%2Fsupply_chain%2FSupplyChainRep_PT.pdf. Acesso em: 10 ago. 2025.

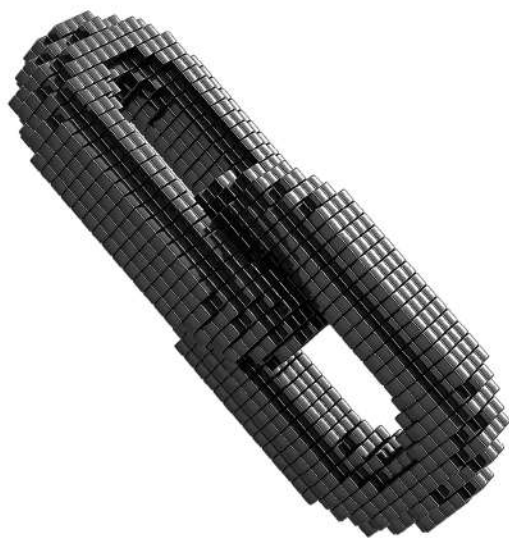
TISCINI, Riccardo; TESTARMATA, Silvia; CIABURRI, Mirella; FERRARI, Emanuele. The blockchain as a sustainable business model innovation. *Management Decision*, v. 58, n. 8, p. 1621–1642, 2020. DOI: 10.1108/MD-09-2019-1281

VERITAS. Governança Social Ambiental: Por que sua marca deve assumir a liderança. Disponível em: <https://www.veritas.com/pt/br/information-center/esg>. Acesso em: 10 ago. 2025.

WALMART Inc.; IBM. *How Walmart brought unprecedented transparency to the food supply chain with Hyperledger Fabric: Case Study*. [S.l.]: The Linux Foundation / Hyperledger, 2018. Disponível em: https://www.lfdecentralizedtrust.org/hubfs/Hyperledger/Printables/Hyperledger_CaseStudy_Walmart_Printable_V4.pdf. Acesso em: 20 nov.2025.

PARTE II

CRIPTOATIVOS, TOKENIZAÇÃO
E CIRCULAÇÃO ECONÔMICA



5. CRIPTOATIVOS E TOKENIZAÇÃO: IMPACTOS JURÍDICOS E TRIBUTÁRIOS NA ESTRUTURA SOCIETÁRIA E COMERCIAL DAS EMPRESAS NO BRASIL

Julianna Ramalho Fonseca

Especialista em Direito Digital pelo Instituto de Tecnologia e Sociedade do Rio de Janeiro – ITS Rio em parceria com o Centro de Estudos e Pesquisas no Ensino do Direito da Universidade do Estado do Rio de Janeiro (CEPED/UERJ). Bacharel em Direito pela Universidade Federal de Pernambuco (UFPE).

INTRODUÇÃO

Vive-se uma revolução digital que reconfigura os fundamentos das relações econômicas e sociais. A emergência da tecnologia *blockchain*, ou tecnologia de registro distribuído (DLT), transcendeu sua aplicação original como infraestrutura da criptomoeda *Bitcoin*, estabelecendo-se como um novo paradigma para a confiança, transparência e eficiência em transações. No cerne dessa transformação, os criptoativos e o processo de tokenização emergem como vetores de inovação disruptiva, impactando diretamente o Direito Empresarial e desafiando os pilares tradicionais do Direito Tributário.

No Brasil, a regulamentação e a utilização desses novos ativos avançam em ritmo acelerado, refletindo mudanças profundas na forma como as empresas estruturam suas operações comerciais, captam recursos e gerenciam suas participações societárias. A introdução desses ativos na estrutura corporativa não apenas oferece oportunidades inéditas de investimento e eficiência operacional, mas também impõe desafios regulatórios e tributários de enorme complexidade.

O arcabouço normativo brasileiro tenta se adaptar a essa “realidade exponencial” (LEITE; SCHWARTZ; FEIGELSON, 2021), gerando um mosaico legislativo composto por normas do Banco

Central (BACEN), da Comissão de Valores Mobiliários (CVM) e da Receita Federal do Brasil (RFB). A promulgação da Lei nº 14.478/2022 (Marco Legal das Prestadoras de Serviços de Ativos Virtuais) e, subsequentemente, da Lei nº 14.754/2023 (Tributação de Aplicações Offshore) redefiniu drasticamente o cenário, criando regimes distintos e, por vezes, conflitantes para operações realizadas no Brasil (*onshore*) e no exterior (*offshore*). A complexidade da tributação da economia digital, marcada pela intangibilidade, volatilidade e transnacionalidade, torna-se evidente (PISCITELLI; SILVEIRA, 2022).

Diante deste panorama, a problemática central desta pesquisa é: como a regulamentação atual e a evolução das normas tributárias para criptoativos e tokenização afetam a estrutura comercial e societária das empresas no Brasil e o que eles representam ao serem adotados?

A hipótese central deste estudo é que, embora a adoção de criptoativos e tokenização ofereça oportunidades significativas para empresas no Brasil, como novas formas de captação de recursos, integralização de capital social e automação de contratos, a falta de regulamentação clara em certas áreas, a fragmentação regulatória entre diferentes órgãos e a complexidade tributária representam desafios substanciais. Argumenta-se que a regulação excessiva ou tecnicamente inadequada, que não compreende o uso prático desses ativos, é capaz de gerar insegurança jurídica, prejudicando a competitividade e a conformidade fiscal das empresas brasileiras.

Para investigar esta hipótese, o presente trabalho adota uma metodologia qualitativa, baseada na revisão bibliográfica de doutrina especializada em Direito Digital, Societário e Tributário, e na análise documental da legislação, normas infralegais (IN RFB nº 1.888/2019), pareceres de orientação (CVM Parecer nº 40) e projetos de lei.

O objetivo geral é analisar os impactos jurídicos e tributários da utilização de criptoativos e tokenização na estrutura societária e comercial das empresas no Brasil. Especificamente, busca-se: (i) examinar os fundamentos técnicos da *blockchain* e dos criptoativos; (ii) analisar o enquadramento regulatório da CVM e do BACEN; (iii) avaliar os impactos da Lei nº 14.478/2022; (iv) identificar os desafios

societários ao se combinar direito societário e esse assunto, como a integralização de capital em criptoativos; e (v) detalhar as complexas implicações tributárias federais, estaduais e municipais.

Este artigo está estruturado em seis capítulos de desenvolvimento. O primeiro capítulo aborda os conceitos fundamentais de criptoativos, *blockchain* e tokenização, bem como a classificação dos *tokens*. O segundo analisa o panorama regulatório nacional e internacional, focando na atuação da CVM, BACEN e RFB. O terceiro capítulo explora os impactos jurídicos diretos na estrutura societária, incluindo a governança e o uso de *smart contracts*. O quarto capítulo dedica-se à análise aprofundada dos aspectos tributários, dissecando as obrigações acessórias (IN RFB nº 1.888/2019) e a bifurcação dos regimes de imposto de renda *onshore* (GCAP) e *offshore* (Lei 14.754/2023). Os capítulos quinto e sexto discutem as possibilidades comerciais, como a tokenização de recebíveis, e as perspectivas futuras, respectivamente. Por fim, as considerações finais sintetizam os achados, validando a hipótese e propondo reflexões sobre a necessidade de harmonização regulatória.

1. CRIPTOATIVOS E TOKENIZAÇÃO: CONCEITOS E FUNDAMENTOS

A compreensão dos impactos jurídicos dos criptoativos exige, primeiramente, a desmistificação de sua base tecnológica e conceitual. Embora frequentemente associados exclusivamente à especulação financeira, sua relevância reside na infraestrutura subjacente: a *blockchain*.

Definição e Características dos Criptoativos

Historicamente, as trocas comerciais evoluíram do escambo para o uso de moedas fiduciárias (FIAT), cuja circulação e valor são controlados por instituições financeiras e bancos centrais, que atuam como intermediários necessários para garantir a confiança. A inovação proposta em 2008 por Satoshi Nakamoto, com o Bitcoin, foi a criação de um sistema de dinheiro eletrônico *peer-to-peer* que elimina a necessidade desse intermediário confiável (SANAS, 2021).

No Brasil, a definição legal mais utilizada para fins regulatórios provém da Instrução Normativa (IN) da Receita Federal nº 1.888, de 2019. Segundo seu Art. 5º, I, um criptoativo é:

a representação digital de valor denominada em sua própria unidade de conta, cujo preço pode ser expresso em moeda soberana local ou estrangeira, transacionado eletronicamente com a utilização de criptografia e de tecnologias de registros distribuídos, que pode ser utilizado como forma de investimento, instrumento de transferência de valores ou acesso a serviços, e que não constitui moeda de curso legal.

Essa definição é fundamental, pois estabelece três pontos-chave: (i) é uma representação digital de valor; (ii) utiliza criptografia e DLT (*blockchain*) ; e (iii) não é moeda de curso legal , sendo, para fins fiscais e cíveis, tratado como um bem intangível. A Lei nº 14.478/2022, de forma similar, em seu artigo 3º, define ativo virtual como “a representação digital de valor que pode ser negociada ou transferida por meios eletrônicos e utilizada para realização de pagamentos ou com propósito de investimento”, excluindo moedas fiduciárias e valores mobiliários tradicionais.

Tecnologia Blockchain e a Base da Tokenização

A *blockchain*, ou tecnologia de registro distribuído (DLT), é a infraestrutura que permite a existência dos criptoativos. Trata-se de um banco de dados descentralizado, no qual as informações (transações) são agrupadas em blocos que, por sua vez, são conectados criptograficamente em uma cadeia.

Seus principais atributos relevantes para o Direito Empresarial são (SANAS, 2021):

1. Descentralização - o registro não é controlado por uma única entidade (como um banco ou um cartório), mas distribuído entre múltiplos participantes (nós) da rede;

2. Imutabilidade - uma vez que um bloco é validado e adicionado à cadeia (através de um mecanismo de consenso, como o *Proof-of-Work*

ou *Proof-of-Stake*), é computacionalmente inviável alterá-lo ou removê-lo, garantindo a integridade histórica do registro;

3. Transparência e Rastreabilidade - embora os participantes possam usar pseudônimos (endereços alfanuméricos), todas as transações registradas na *blockchain* são, em geral, públicas e auditáveis por qualquer membro da rede.

É essa capacidade de criar registros digitais únicos, seguros e imutáveis que permite a tokenização. Tokenizar é o processo de representar digitalmente um ativo (real ou intangível) ou a propriedade sobre ele em uma *blockchain*. Um *token* é, portanto, a grosso modo, a representação digital desse direito ou ativo, podendo, em alguns casos, se estabelecer como um criptoativo, observada a definição presente no subcapítulo 1.1. e o disposto no subcapítulo 1.3 deste trabalho e que nem todos os *tokens* são criptoativos, mas todo o criptoativo é um *token*.

Como aponta Costa (2021), a tokenização difere da securitização tradicional. Enquanto a securitização transforma direitos creditórios em valores mobiliários (*securities*) dentro de um arranjo jurídico pré-definido e centralizado, a tokenização estrutura a operação em um arranjo tecnológico descentralizado (a *blockchain*), permitindo a negociação global e supraestatal desses ativos.

Classificação de Tokens: Utilitários, de Pagamento e de Segurança

A amplitude da definição de criptoativo abarca diferentes naturezas de tokens, cuja classificação é essencial para determinar o regime jurídico e tributário aplicável. A doutrina e os reguladores internacionais (como a ESMA e a SEC) costumam classificá-los em três grandes grupos (COSTA, 2021):

- Tokens de Pagamento (*Payment Tokens* ou Criptomoedas): São aqueles cujo objetivo principal é servir como meio de troca ou reserva de valor, funcionando de forma análoga a uma moeda, embora sem curso legal. O *Bitcoin* (BTC) e o *Ether* (ETH) em sua função primária são os exemplos clássicos.

- Tokens de Utilidade (*Utility Tokens*): Conferem ao seu titular o direito de acesso ou consumo futuro de produtos ou serviços específicos dentro de uma plataforma ou ecossistema digital. Funcionam como uma espécie de cupom digital ou uma ficha de arcade. O detentor não espera um retorno financeiro passivo, mas sim o direito de usar o serviço.
- Tokens de Segurança (*Security Tokens* ou *RWA - Real World Assets*): São a categoria de maior complexidade jurídica. Representam ativos ou direitos econômicos tradicionais, como a participação nos lucros de um empreendimento, direitos de voto, ações de uma empresa, títulos de dívida ou frações de um imóvel. Quando um token confere direitos dessa natureza, ele deixa de ser um simples bem e passa a ser tratado como um valor mobiliário, atraindo a competência regulatória da CVM.

Uma quarta categoria que ganhou proeminência são os Tokens Não Fungíveis (NFTs). Diferentemente dos anteriores (fungíveis, ou seja, intercambiáveis), o NFT é um certificado de propriedade digital único, associado a um bem específico (real ou virtual), como uma obra de arte ou um item colecionável. Juridicamente, o NFT não é o ativo em si, mas um certificado infungível de propriedade digital, cuja unicidade e escassez são garantidas pela blockchain (COSTA, 2021).

Essa distinção é o eixo central da regulação de criptoativos no Brasil, determinando qual autoridade (Banco Central ou CVM) supervisionará a operação e qual regime tributário (Ganho de Capital ou Renda Variável) será aplicado.

2. REGULAÇÃO DE CRIPTOATIVOS NO BRASIL E NO MUNDO

A natureza transnacional dos criptoativos impõe um desafio regulatório global. A regulação eficaz não pode ser puramente doméstica, pois os agentes podem facilmente migrar para jurisdições mais favoráveis, ocorrendo a chamada arbitragem regulatória. O

Brasil tem buscado alinhar seu arcabouço normativo às diretrizes internacionais, notadamente as do Grupo de Ação Financeira (GAFI/FATF) focadas na Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo (PLD/FT).

Panorama Regulatório Internacional

Internacionalmente, observa-se uma fragmentação de abordagens. Os Estados Unidos adotam uma regulação baseada na natureza do ativo, na qual a *Securities and Exchange Commission* (SEC) aplica rigorosamente o Teste de Howey para classificar tokens como *securities* (valores mobiliários), enquanto a *Commodity Futures Trading Commission* (CFTC) supervisiona derivativos de criptoativos como *commodities*.

O referido teste, originário do precedente *SEC v. W.J. Howey Co.* julgado pela Suprema Corte norte-americana em 1946, estabeleceu os critérios para identificar a existência de um contrato de investimento. A metodologia consiste em verificar, cumulativamente, a presença de quatro elementos: (i) o investimento de dinheiro (ou bens suscetíveis de avaliação econômica); (ii) em um empreendimento comum; (iii) com a expectativa de lucros; (iv) a serem obtidos predominantemente pelos esforços do empreendedor ou de terceiros. Na economia digital, a SEC adaptou esse entendimento para buscar a figura do “Participante Ativo” (*Active Participant*), cuja atuação gerencial é determinante para o sucesso do projeto cripto e a consequente valorização do *token*, justificando a incidência das normas de proteção ao investidor.

A União Europeia, por sua vez, aprovou o regulamento *Markets in Crypto-Assets* (MiCA), criando um regime jurídico unificado e abrangente para emissores e prestadores de serviços em todo o bloco, buscando harmonizar o mercado. A Organização para a Cooperação e Desenvolvimento Econômico (OCDE) também tem exercido papel crucial, não apenas na esfera tributária (com os projetos BEPS e o *Crypto-Asset Reporting Framework* - CARF), mas também ao analisar o impacto da tokenização nos mercados financeiros.

A dificuldade regulatória reside no fato de que a tecnologia *blockchain* permite a criação de uma governança tecnológica descentralizada, por vezes referida como *lex mercatoria ex machina*, onde as regras são embutidas no próprio código (*code is law*), desafiando a soberania regulatória estatal tradicional.

Enquadramento Jurídico no Brasil: A Lei nº 14.478/2022

No Brasil, o amadurecimento do arcabouço regulatório sobre a criptoeconomia foi fruto de um extenso debate legislativo, iniciado em 2015 com o Projeto de Lei (PL) nº 2.303/2015. Esse processo culminou na promulgação da Lei nº 14.478, de 21 de dezembro de 2022 (originada do PL nº 4.401/2021), conhecida como o Marco Legal dos Criptoativos.

É crucial compreender o escopo desta legislação: ela não regula o criptoativo em si (o *token* ou a moeda), mas sim as Prestadoras de Serviços de Ativos Virtuais (PSAVs), internacionalmente conhecidas como VASPs (*Virtual Asset Service Providers*) e popularmente chamadas de *exchanges*. A lei define a PSAV como a pessoa jurídica que executa, em nome de terceiros, serviços como troca (moeda fiduciária por criptoativo, ou entre criptoativos), transferência, custódia ou administração de ativos virtuais.

Ainda, assim os principais pilares estabelecidos pela Lei nº 14.478/2022 e contribuições para a regulamentação brasileira dos criptoativos foram:

- Designação do Regulador: A lei atribuiu ao Poder Executivo a faculdade de indicar o órgão regulador, tendo sido o Banco Central do Brasil (BCB) o escolhido para autorizar e supervisionar o funcionamento das PSAVs no país (Decreto nº 11.563/2023);
- Regras de PLD/FT: Alinhando-se às recomendações do GAFI (*Grupo de Ação Financeira Internacional*), a lei incluiu as PSAVs no rol de entidades obrigadas a cumprir as diretrizes da Lei nº 9.613/1998 (Lei de Lavagem de Dinheiro), devendo

monitorar transações e reportar operações suspeitas ao Conselho de Controle de Atividades Financeiras (COAF);

- Proteção ao Consumidor: As operações com ativos virtuais foram expressamente submetidas às normas do Código de Defesa do Consumidor (CDC);
- Tipos Penais: Houve a criação de um tipo penal específico no Código Penal (art. 171-A) para a “fraude com a utilização de ativos virtuais, valores mobiliários ou ativos financeiros”, visando coibir pirâmides financeiras e golpes no setor.

Ainda assim, embora a Lei de 2022 tenha estabelecido as diretrizes gerais, a operacionalização do mercado dependia da regulamentação infralegal pelo órgão competente, até por lacunas que a própria lei em questão deixou para isso. Esse vácuo foi preenchido em novembro de 2025, quando o Banco Central publicou as normas definitivas que regulam os serviços de ativos virtuais no Brasil: as Resoluções BCB nº 519, 520 e 521/2025, além da Resolução Conjunta CMN/BC nº 14/2025.

Essas normas, que entram em vigor majoritariamente em fevereiro de 2026, trouxeram rigor e institucionalização ao setor, com destaque para:

1. Segregação Patrimonial Mandatória: Diferente do texto original da lei, que deixava margem para interpretação, as novas resoluções tornam obrigatória a separação entre o patrimônio da empresa e os ativos dos clientes. Os recursos (seja em cripto ou reais) devem ser mantidos em contas individualizadas de depósito ou pagamento em nome dos clientes, mitigando riscos de confusão patrimonial em casos de insolvência da plataforma.

2. Requisitos de Capital e Governança: A Resolução Conjunta estabeleceu uma régua elevada para a entrada e manutenção das empresas no mercado. O patrimônio líquido mínimo exigido para as PSAVs varia entre R\$ 10,8 milhões e R\$ 37,2 milhões, dependendo da complexidade da atividade exercida. Esse montante, significativamente superior ao exigido em outras jurisdições (como na União Europeia sob

o regulamento MiCA), sinaliza uma opção do regulador pela robustez e solvência, o que tenderá a gerar uma consolidação do mercado, dificultando a sobrevivência de *players* menores sem aporte de capital institucional.

3. Tratamento das *Stablecoins* e Câmbio: As operações com *stablecoins* pareadas a moedas fiduciárias (como o dólar) e as transferências internacionais de criptoativos foram enquadradas na sistemática do mercado de câmbio. Isso implica a obrigatoriedade de reporte ao Banco Central e abre precedentes para a futura incidência de Imposto sobre Operações Financeiras (IOF).

4. Presença Física para Estrangeiras: As normas impõem barreiras para *exchanges* transfronteiriças que operam remotamente. Para atender clientes brasileiros, as empresas estrangeiras deverão constituir operação local com sede física (vedado o uso de escritórios virtuais) e obter a licença de PSAV junto ao BC, ou estabelecer parcerias com entidades locais reguladas.

Portanto, essa evolução do cenário jurídico brasileiro sinaliza uma guinada em direção a um modelo de excessiva intervenção estatal. Sob o pretexto da segurança jurídica e da prevenção à lavagem de dinheiro, superou-se o estado de um ambiente de elevada incerteza, mas instituiu-se um aparato de vigilância incompatível com a natureza da tecnologia, como demonstra a exigência de identificação de beneficiários até em transferências para carteiras de autocustódia. Tal postura ergue barreiras de entrada proibitivas que sufocam a inovação descentralizada, descaracterizam a essência da criptoeconomia e favorecem a concentração de mercado nas mãos de intermediários tradicionais, em detrimento da livre iniciativa e do desenvolvimento de soluções genuinamente disruptivas.

A Atuação Fragmentada: CVM, Banco Central e Receita Federal

O ecossistema regulatório brasileiro é, portanto, tripartite, com competências distintas e, por vezes, sobrepostas:

1. Banco Central (BACEN): Regula as *prestadoras de serviço* (VASPs), focando na estabilidade do sistema financeiro, PLD/FT e regras de autorização de funcionamento, conforme a Lei 14.478/2022.

2. Receita Federal (RFB): Regula a *obrigação tributária*. Através da IN 1888/2019, define criptoativos para fins fiscais e impõe a obrigação acessória de reporte de operações, como será detalhado no Capítulo 4 deste trabalho.

3. Comissão de Valores Mobiliários (CVM): Regula o *ativo*, quando este é um valor mobiliário (*security token*).

A atuação da CVM é o ponto de maior complexidade jurídica para as empresas. A Lei 14.478/2022 explicitamente *não* alterou as competências da CVM. A CVM, através do Parecer de Orientação nº 40/2022 (e em linha com manifestações anteriores), consolidou seu entendimento de que um criptoativo (incluindo NFTs) será considerado um valor mobiliário se preencher os requisitos do “Teste de Howey”, conforme explicado no Subcapítulo 2.1. deste trabalho, em uma versão adaptada da jurisprudência norte-americana, verificando se o ativo configura um Contrato de Investimento Coletivo (CIC), nos termos do Art. 2º, IX, da Lei nº 6.385/1976

Se um token for classificado como valor mobiliário (ex: um token que promete participação nos lucros futuros de uma safra de soja tokenizada, ou de um empreendimento imobiliário), sua oferta pública exige registro prévio (ou dispensa) na CVM, sob pena de ser considerada uma oferta irregular. Esta classificação tem implicações societárias (regras de *disclosure* e governança) e tributárias (como será visto no Capítulo 4 deste trabalho) radicalmente distintas daquelas aplicáveis aos *utility tokens* ou criptomoedas.

3. IMPACTOS JURÍDICOS E SOCIETÁRIOS DA TOKENIZAÇÃO

A tokenização e as tecnologias associadas (DLT e *smart contracts*) não alteram apenas o mercado financeiro, mas impactam também o núcleo do Direito Societário e Comercial, modificando a forma

como empresas são capitalizadas, gerenciadas e como executam suas obrigações.

Efeitos na Estrutura Societária e o Desafio da Integralização de Capital

O impacto societário mais direto e já consolidado no Brasil é a possibilidade de integralização de capital social com criptoativos. Por muito tempo, houve dúvida se criptomoedas poderiam ser usadas para este fim, visto que o capital social deve ser expresso em moeda corrente (Real) e integralizado com dinheiro ou “bens suscetíveis de avaliação pecuniária” (Art. 997, III, CC; Art. 7º, LSA) .

A questão foi resolvida pelo Departamento Nacional de Registro Empresarial e Integração (DREI), através do Ofício Circular SEI nº 4081/2020. O DREI firmou o entendimento de que:

- Não há vedação legal expressa para a integralização de capital com criptomoedas.
- Criptoativos são bens incorpóreos que possuem avaliação pecuniária (valor de mercado), enquadrando-se, portanto, no conceito de “bem” exigido pela legislação.
- O registro do ato societário (contrato social ou alteração) na Junta Comercial deve seguir as mesmas regras da integralização com bens móveis.

Essa possibilidade abre um novo vetor de captação para *startups* e empresas de tecnologia. Contudo, ela traz um desafio prático de *valuation* e responsabilidade. Dada a alta volatilidade dos criptoativos, a avaliação pecuniária (requisito legal) torna-se complexa. Se um sócio integraliza R\$ 100.000,00 em Bitcoin e o valor do ativo cai 50% no dia seguinte, o capital social real foi corroído.

Nesse cenário, a responsabilidade dos sócios (na sociedade limitada) ou dos avaliadores (na sociedade anônima) é crucial. No caso das limitadas, os sócios respondem solidariamente pela exatidão da avaliação dos bens (Art. 1.055, § 1º, CC). Na prática, as Juntas

Comerciais têm exigido um laudo de avaliação emitido por perito ou empresa especializada, que ateste o valor em Reais do criptoativo na data da integralização, mitigando o risco, mas não eliminando o problema da volatilidade pós-integralização.

Contratos Inteligentes (Smart Contracts) versus Registro Empresarial

Os *smart contracts* (contratos inteligentes), conceito cunhado por Nick Szabo em 1994, são programas de computador (códigos) que executam automaticamente os termos de um contrato quando condições pré-definidas são atendidas. Quando implementados em uma *blockchain* (como a Ethereum), eles herdam suas características de imutabilidade e descentralização.

Do ponto de vista jurídico, *smart contracts* não são uma nova espécie contratual, mas sim uma nova *forma* de execução de um negócio jurídico. Seu potencial empresarial reside na automação de processos, redução de custos de transação e mitigação do risco de inadimplemento.

Apesar da eficiência, a adoção de *smart contracts* e da tokenização em estruturas societárias formais enfrenta um desafio central: o registro público.

Atos societários que alteram a estrutura da empresa (como a transferência de quotas ou ações, fusões, cisões) exigem, para sua plena validade *erga omnes*, o arquivamento na Junta Comercial. O DREI, através da IN nº 81/2020, regula o formato desses atos, que devem ser submetidos em língua portuguesa e em formato de documento digital (PDF/A).

O problema surge porque a linguagem de programação de um *smart contract* não é o formato aceito pelas Juntas Comerciais. Não é possível, hoje, “registrar” um *smart contract* que transfere automaticamente a titularidade de quotas na Junta Comercial. A transferência efetiva ainda depende da submissão do ato societário tradicional.

Portanto, a aplicação societária da *blockchain* para atos societários no Brasil encontra-se em um modelo híbrido:

1. Atos *Inter Partes* (Privados): *Smart contracts* são plenamente viáveis para regular obrigações que não exigem registro público, como acordos de acionistas ou cotistas, onde as regras de voto ou preferência podem ser automatizadas entre os signatários.

2. Atos *Erga Omnes* (Públicos): A *blockchain* e os *smart contracts* podem servir como plataforma de execução (ex: para o pagamento em uma operação de M&A), mas a eficácia societária da transferência de propriedade (quotas/ações) ainda depende do registro do ato societário tradicional na Junta Comercial.

Compliance e Desafios Regulatórios para a Governança

A utilização de *smart contracts* também levanta questões sobre a autonomia da vontade e a revisão judicial. A premissa *code is law*, onde o contrato é autoexecutável e imutável, colide com princípios basilares do Direito Contratual brasileiro, como a função social do contrato (Art. 421, CC), a boa-fé objetiva (Art. 422, CC) e a possibilidade de revisão por onerosidade excessiva (Art. 478, CC).

Se um *smart contract* executa automaticamente uma cláusula que, à luz do caso concreto, mostra-se abusiva ou ilegal (por exemplo, violando o CDC, que é aplicável às VASPs), surge um conflito. A imutabilidade tecnológica não pode se sobrepor à inafastabilidade da jurisdição.

Ademais, no âmbito da governança corporativa, a tokenização pode levar à criação das *Decentralized Autonomous Organizations* (DAOs), organizações geridas por regras embutidas em *smart contracts* e controladas por detentores de tokens de governança. Essas estruturas desafiam o modelo societário tradicional (LTDA, S.A.), pois muitas vezes carecem de uma administração centralizada e de um registro formal, gerando um vácuo de responsabilidade civil e regulatória que o Direito brasileiro ainda não endereçou.

4. COMPLIANCE E DESAFIOS REGULATÓRIOS PARA A GOVERNANÇA

O capítulo mais complexo da adoção de criptoativos por empresas e pessoas físicas é, sem dúvida, o tributário. O Brasil desenvolveu um regime fiscal bifurcado, onde a localização da custódia do ativo (Brasil ou exterior) define integralmente o método de apuração e a incidência de isenções.

Os Desafios da Tributação na Economia Digital Exponencial

A “tributação da economia digital” (PISCITELLI; SILVEIRA, 2022) não é um problema novo. A OCDE debate o tema há mais de duas décadas, desde a Conferência de Ottawa em 1998, focando nos desafios da intangibilidade, da ausência de presença física e das operações transfronteiriças. A tokenização e os criptoativos representam uma “realidade exponencial” (LEITE; SCHWARTZ; FEIGELSON, 2021) que agrava esses desafios, pois a descentralização da *blockchain* remove os intermediários financeiros tradicionais que historicamente atuaram como agentes de retenção e informação para o Fisco.

A legislação tributária brasileira, concebida na era analógica (MACHADO SEGUNDO, 2020), enfrenta dificuldades estruturais para classificar esses novos eventos: a mineração é “mercadoria” (ICMS) ou “serviço” (ISS)? A permuta de tokens é “alienação”? A quem imputar a responsabilidade tributária em uma transação *peer-to-peer* (P2P) global?. A resposta do Fisco brasileiro tem sido focar na vigilância dos pontos de conversão para moeda fiduciária.

A Obrigação Acessória: IN RFB nº 1.888/2019 e o Reporte de Operações

A principal ferramenta de fiscalização da Receita Federal é a IN 1888/2019, uma obrigação acessória (dever de informar) que antecede a obrigação principal (pagar o imposto).

A norma impõe o dever de reportar mensalmente as operações com criptoativos a dois sujeitos distintos:

1. Exchanges Domiciliadas no Brasil (Art. 6º, I): Devem reportar à RFB a totalidade das operações de todos os seus usuários (pessoas físicas e jurídicas), incluindo saldos e identificação.

2. Pessoas Físicas ou Jurídicas (Art. 6º, II): O próprio contribuinte deve reportar suas operações, via sistema Coleta Nacional no e-CAC, nos seguintes casos:

Se as operações forem realizadas em exchange domiciliada no exterior; ou Se as operações não forem realizadas em exchange (ex: transações P2P, *hot* ou *cold wallets* próprias).

O gatilho para a obrigatoriedade de declaração pelo próprio contribuinte (Art. 6º, II) ocorre apenas se o valor mensal total das operações (soma de compras, vendas, permutas, etc.) ultrapassar R\$ 30.000,00 (trinta mil reais).

Crucialmente, a IN 1888/2019 exige o reporte de “permuta” (troca de um criptoativo por outro, ex: BTC por ETH). Este dispositivo é a base normativa que sustenta o entendimento da RFB de que a permuta é um fato gerador de ganho de capital, pois configura uma “alienação” (disposição de um bem) que deve ser tributada no momento da troca, e não apenas na conversão final para Reais. Para empresas, essa interpretação gera enorme complexidade contábil, exigindo a apuração de ganho de capital em milhares de transações *crypto-to-crypto* diárias.

A Bifurcação do Imposto de Renda: Regimes Onshore vs. Offshore

Desde 1º de janeiro de 2024, vigora no ordenamento jurídico brasileiro uma divisão estrutural no regime de tributação do Imposto de Renda da Pessoa Física (IRPF) incidente sobre criptoativos, baseada na localização da custódia dos ativos. No que tange ao denominado Regime *Onshore*, aplicável aos ativos mantidos em *exchanges* brasileiras (VASPs) ou em carteiras próprias em território nacional, a natureza jurídica fiscal permanece atrelada ao conceito de “outros bens” ou “ativo financeiro”, seguindo, na prática, a regulação de bens móveis.

O fato gerador constitui-se no ganho de capital auferido na alienação, seja por venda ou permuta.

Neste regime doméstico, a regra de isenção prevista no Art. 22 da Lei nº 9.250/1995 permanece como ponto central: os ganhos de capital são isentos de IRPF se o valor total das alienações realizadas no mês for inferior a R\$ 35.000,00. Importa destacar que, embora a Medida Provisória nº 1.303/2025 tenha tentado revogar tal benefício, a norma perdeu sua eficácia ao não ser convertida em lei pelo Congresso Nacional em 09 de outubro de 2025. Consequentemente, a isenção mantém-se em plena vigência. Para alienações que excedam esse limite, aplica-se a tributação sobre o ganho de capital mediante alíquotas progressivas (15% a 22,5%), conforme disposto no Art. 21 da Lei nº 8.981/95.

Em contrapartida, o Regime *Offshore*, disciplinado pela Lei nº 14.754/2023, impõe tratamento distinto aos ativos custodiados no exterior. A legislação reclassificou expressamente os “ativos virtuais” e “carteiras digitais” no exterior como “aplicações financeiras” (Art. 3º, § 1º, I), englobando em seus rendimentos a variação cambial e da criptomoeda frente à moeda nacional. A principal consequência dessa reclassificação é a inaplicabilidade da isenção de R\$ 35.000,00, típica dos “bens”. A apuração passa a ser anual e consolidada (Art. 2º), com tributação do resultado líquido positivo na Declaração de Ajuste Anual (DAA) à alíquota única de 15%, permitindo-se a compensação de perdas com ganhos de outras aplicações financeiras no exterior dentro do mesmo exercício (Art. 9º). A lei também pacificou a transparência fiscal dos *trusts* no exterior (Art. 10), mantendo os bens sob titularidade do instituidor para fins fiscais até a distribuição .

Essa bifurcação normativa estabelece uma “tributação geográfica”, criando incentivos regulatórios para o uso de plataformas nacionais reguladas pelo BACEN, o que, por sua vez, assegura à Receita Federal o recebimento automático de informações pelo fluxo estabelecido na IN RFB nº 1.888/2019.

Por fim, deve-se observar a especificidade dos *Security Tokens*. Caso um token (fungível ou NFT) seja caracterizado como valor

mobiliário pela CVM, afasta-se tanto o regime de ganho de capital quanto o de aplicação financeira internacional, incidindo as regras de Renda Variável. Nesse cenário, não se aplica a isenção de R\$ 35.000,00 (própria de bens), nem a isenção de R\$ 20.000,00 (exclusiva para ações no mercado à vista). A tributação ocorre mediante alíquotas de 15% sobre o ganho líquido em operações comuns e 20% em *day trade*, com apuração e recolhimento mensal via DARF (código 6015). Já para as Pessoas Jurídicas, independentemente do regime (Lucro Real ou Presumido), os criptoativos devem ser classificados contabilmente conforme sua destinação (caixa, investimento ou intangível), sendo os ganhos tributados como receita ou lucro, sujeitando-se à incidência de IRPJ e CSLL.

Desafios Fiscais Estaduais (ICMS/ITCMD) e Municipais (ISS)

A complexidade tributária dos criptoativos transcende a esfera federal, irradiando efeitos para as competências estaduais e municipais. No âmbito estadual, a classificação jurídica dos criptoativos como bens intangíveis enseja a incidência do Imposto sobre Transmissão Causa Mortis e Doação (ITCMD). A transmissão não onerosa desses ativos, seja por ato *inter vivos* (doação) ou *causa mortis* (herança), configura o fato gerador do tributo, cuja base de cálculo deve refletir o valor de mercado dos ativos na data da transmissão.

Paralelamente, a incidência do Imposto sobre Circulação de Mercadorias e Serviços (ICMS) representa um dos pontos de maior insegurança jurídica no setor. A controvérsia doutrinária, destacada por Machado Segundo (2020), reside na tipificação da atividade de mineração e validação de transações: questiona-se se tal atividade configuraria circulação de mercadoria digital, atraindo a competência estadual (ICMS), ou prestação de serviço de processamento de dados, atraindo a competência municipal (ISS). Dada a intangibilidade e a natureza *sui generis* dos criptoativos, a doutrina majoritária tende a afastar a incidência do ICMS, por faltar-lhe o pressuposto material de “mercadoria”.

Em contrapartida, a competência municipal apresenta contornos mais definidos. A Lei nº 14.478/2022 e a IN RFB nº 1.888/2019 caracterizam as *exchanges* (VASPs) inequivocamente como prestadoras de serviços. Dessa forma, as atividades de intermediação, corretagem, custódia e administração de ativos virtuais constituem fatos geradores do Imposto Sobre Serviços (ISS), tributo devido ao município do estabelecimento do prestador. A incidência do imposto abrange, ainda, as empresas de tecnologia dedicadas ao desenvolvimento de *smart contracts* ou plataformas de tokenização, enquadradas na prestação de serviços de desenvolvimento de *software* e processamento de dados.

5. OPORTUNIDADES E DESAFIOS COMERCIAIS NA UTILIZAÇÃO DE CRIPTOATIVOS

A infraestrutura regulatória e fiscal, embora complexa, pavimentou o caminho para a adoção empresarial dos criptoativos, que se movem da especulação para a utilidade comercial. A tokenização, em particular, representa uma transformação significativa na gestão de ativos e captação de recursos.

*Adoção Corporativa e a Gestão de Tesouraria**

Empresas no Brasil e no mundo começam a adotar criptoativos (majoritariamente Bitcoin e *stablecoins*) como parte de sua estratégia de gestão de tesouraria. Esta prática serve como *hedge* (proteção) contra a inflação da moeda fiduciária ou como um ativo de investimento de longo prazo.

No entanto, essa adoção impõe desafios contábeis e fiscais significativos. A volatilidade exige marcação a mercado constante, e os ganhos de capital (no caso de PJs) entram na base de cálculo do IRPJ e da CSLL, como melhor explicado no capítulo anterior deste trabalho. A falta de normas contábeis específicas (CPCs) para criptoativos no Brasil obriga as empresas a se guiarem por analogia (ativos intangíveis ou instrumentos financeiros), gerando insegurança na auditoria das demonstrações financeiras.

Tokenização de Ativos do Mundo Real (RWA): Imóveis e Recebíveis

No cenário econômico contemporâneo, a tokenização de Ativos do Mundo Real (*Real World Assets* - RWA) desponta como uma das fronteiras mais promissoras para a inovação comercial. A tecnologia *blockchain* viabiliza o fracionamento digital de ativos historicamente caracterizados pela iliquidez - como imóveis, obras de arte, precatórios e recebíveis, permitindo sua negociação em mercados globais com níveis superiores de liquidez e transparência.

Especificamente no setor imobiliário, a tokenização propicia a aquisição de frações ideais de propriedade ou de direitos sobre fluxos de rendimentos, como aluguéis. Todavia, a plena eficácia jurídica desse modelo enfrenta o óbice da formalidade registral: a transferência da propriedade imobiliária permanece condicionada ao registro no Cartório de Registro de Imóveis (RGI). Tal instituição, à semelhança das Juntas Comerciais, ainda carece de integração com as tecnologias de registro distribuído (DLT), gerando um descompasso entre a velocidade da transação digital e a morosidade do registro público.

No âmbito dos recebíveis e da renda fixa, a emissão de tokens representativos de direitos creditórios (e.g., duplicatas, recebíveis de cartões) ou instrumentos de dívida corporativa emerge como uma alternativa eficiente de financiamento. Esse mecanismo faculta às empresas a antecipação de receitas e a captação direta de recursos (*peer-to-peer*), mitigando os custos de transação inerentes à intermediação bancária tradicional.

Contudo, a operacionalização desses modelos impõe desafios regulatórios e tributários substanciais. Consoante examinado no Capítulo 2.3, a oferta de tokens que prometem fluxos de renda futuros ou participação em resultados tende a ser enquadrada como oferta pública de Contratos de Investimento Coletivo, atraindo a qualificação de *security tokens*. Consequentemente, tais ativos submetem-se à regulação da Comissão de Valores Mobiliários (CVM) e, na esfera fiscal, ao regime de tributação de Renda Variável, o que eleva a complexidade

operacional e os custos de conformidade em comparação à emissão de meros *utility tokens*.

Inovações em Pagamentos e Segurança de Dados

Para o comércio, o uso de criptoativos (especialmente *stablecoins* - tokens lastreados em moeda fiduciária) como meio de pagamento oferece vantagens em transações internacionais, reduzindo custos e tempo de compensação bancária (SWIFT). A Lei 14.478/2022, ao prever a regulação dos “serviços de pagamento” pelo BACEN, abre caminho para que as criptomoedas sejam formalmente integradas ao Sistema de Pagamentos Brasileiro (SPB).

No âmbito da segurança de dados, a *blockchain* pode ser usada para criar sistemas de identidade digital soberana (SSI), onde o usuário (cliente) controla seus próprios dados, alinhando-se aos princípios da LGPD, embora a implementação ainda seja incipiente.

6. PERSPECTIVAS FUTURAS E IMPACTOS NA COMPETITIVIDADE EMPRESARIAL

O cenário de criptoativos e tokenização está em constante evolução, e a competitividade das empresas brasileiras dependerá de sua capacidade de adaptação a este novo paradigma tecnológico e regulatório.

O Potencial Transformador dos Criptoativos e da Tokenização

O potencial transformador reside na desintermediação e na eficiência. A automação via *smart contracts* (Capítulo 3, em especial o Subcapítulo 3.2) reduz custos operacionais e de agência. A tokenização (Capítulo 5, em especial o Subcapítulo 5.2) cria liquidez para ativos ilíquidos e abre novos mercados de captação. Para que esse potencial seja plenamente realizado, é imperativo que o arcabouço jurídico ofereça segurança e clareza.

A “realidade exponencial” (LEITE; SCHWARTZ; FEIGELSON, 2021) da economia digital exige que o Direito acompanhe a tecnologia.

A governança de empresas tokenizadas (DAOs) , a responsabilidade civil por falhas em *smart contracts* e a proteção do consumidor em ambientes descentralizados são fronteiras que o Direito brasileiro apenas começou a explorar.

Adaptação do Mercado e Novas Estratégias Empresariais

As empresas brasileiras enfrentam a necessidade estratégica de compreender este ecossistema. Isso envolve não apenas avaliar o uso de criptoativos como caixa (*treasury*), mas como ferramenta de capitalização (integralização de capital) e de estruturação de novos produtos (tokenização de RWA).

A estratégia comercial, contudo, é diretamente impactada pelos desafios regulatórios. Como aponta Costa, a regulação focada apenas em *exchanges* nacionais (Lei 14.478/2022) cria uma assimetria competitiva. Empresas estrangeiras que operam sem sede no Brasil (e que, portanto, não reportam automaticamente à RFB via IN 1888/2019) atraem usuários que buscam maior privacidade.

Contudo, a Lei 14.754/2023 age como um contrapeso: embora a VASP *offshore* não reporte, o *usuário* agora possui um regime tributário (o *offshore*) potencialmente menos vantajoso (sem a isenção dos R\$ 35.000,00). A competitividade, portanto, está atrelada à forma como a regulação (BACEN) e a fiscalização (RFB) conseguirão atuar sobre esses agentes *offshore* e como os contribuintes perceberão o custo-benefício de cada regime.

Reflexões sobre “Mineração Verde”, Regulação e Economia Digital

Uma crítica frequente aos criptoativos, especialmente ao Bitcoin, é o alto consumo de energia de seu mecanismo de consenso (*Proof-of-Work*). Ciente disso, o legislador brasileiro inseriu na Lei nº 14.478/2022 (Art. 15, no substitutivo do PL 4.401/2021) incentivos fiscais federais (alíquota zero de PIS, COFINS, IPI e Imposto de Importação) para a aquisição de hardware e software destinados à mineração, com uma condição clara: que a empresa utilize “100% de sua necessidade

de energia elétrica de fontes renováveis” e neutralize 100% de suas emissões de gases de efeito estufa.

Esta medida é uma perspectiva futura crucial para o Brasil. Estados com alta capacidade de geração de energia limpa (como a eólica e solar no Nordeste, ou hidrelétrica em outras regiões) podem se tornar polos globais de “mineração verde”, atraindo investimentos internacionais e posicionando o país como um líder em uma criptoeconomia sustentável.

A regulação, portanto, não deve ser vista apenas como um freio, mas como um indutor de boas práticas e um alinhador da inovação tecnológica com metas de sustentabilidade (ESG), essenciais para a competitividade empresarial no século XXI.

CONSIDERAÇÕES FINAIS

Este trabalho de conclusão de curso analisou os complexos impactos jurídicos e tributários decorrentes da adoção de criptoativos e da tokenização por empresas no Brasil, um campo marcado pela rápida inovação tecnológica e por um arcabouço regulatório em plena formação.

A pesquisa permitiu confirmar a hipótese central: os criptoativos e a tokenização representam uma oportunidade disruptiva para o Direito Empresarial, mas sua implementação é obstada por uma significativa insegurança jurídica e complexidade fiscal. A “tributação da economia digital” (PISCITELLI; SILVEIRA, 2022) e a “realidade exponencial” (LEITE; SCHWARTZ; FEIGELSON, 2021) desafiam os conceitos tradicionais de fato gerador, territorialidade e responsabilidade tributária (MACHADO SEGUNDO, 2020).

No plano societário, a inovação é tangível. A permissão do DREI para a integralização de capital social com criptoativos (Ofício Circular SEI nº 4081/2020) é um marco que oferece novas estruturas de capitalização. Contudo, essa modernidade encontra barreiras no registro público: a rigidez das Juntas Comerciais, ainda baseadas em documentos textuais (IN DREI nº 81/2020), impede a plena utilização

de *smart contracts* para atos societários que demandam arquivamento , relegando-os a um papel de execução de obrigações privadas (como acordos de acionistas).

No plano regulatório, o Brasil avançou ao definir as competências com a Lei nº 14.478/2022, um progresso que se consolidou em novembro de 2025 com a publicação do arcabouço infralegal definitivo pelo Banco Central (Resoluções BCB nº 519, 520 e 521 e Resolução Conjunta CMN/BC nº 14). Essas normas operacionalizaram a supervisão estatal sobre as *exchanges* (PSAVs), impondo requisitos robustos de capital e governança com foco na estabilidade e na prevenção à lavagem de dinheiro (PLD/FT). Paralelamente, a CVM mantém sua competência sobre os *security tokens*, aplicando o “Teste de Howey” (Parecer de Orientação nº 40) para identificar contratos de investimento coletivo. Essa fragmentação, agora densamente regulada em ambas as frentes, exige alta especialização das empresas para classificar corretamente seus *tokens* e navegar entre as exigências prudenciais do BACEN e as regras de oferta pública da CVM, mitigando o risco de irregularidade.

O maior desafio, contudo, reside na esfera tributária. A RFB, através da IN 1888/2019, criou um robusto sistema de vigilância (obrigação acessória), especialmente ao considerar a permuta como fato gerador. Mais recentemente, a Lei nº 14.754/2023 estabeleceu uma bifurcação radical no Imposto de Renda:

1. Operações *Onshore*: Permanecem como “outros bens”, gozando da isenção de ganho de capital para alienações mensais de até R\$ 35.000,00 (Lei nº 9.250/1995), benefício que sobreviveu à tentativa de revogação pela MP 1.303/2025;

2. Operações *Offshore*: São reclassificadas como “aplicações financeiras”, perdendo a isenção e sendo submetidas a uma alíquota única de 15% sobre o ganho anual consolidado.

Esta estrutura cria uma “tributação geográfica”, incentivando o uso de plataformas nacionais reguladas pelo BACEN, mas aumentando a complexidade do *compliance* para investidores globais. Nas esferas estadual e municipal, ainda pairam incertezas sobre o

ICMS (mineração) e oportunidades claras no ISS (incentivos como o do Porto Digital).

Conclui-se que, para o Brasil capitalizar o potencial da criptoeconomia, fomentando a competitividade empresarial e a inovação (como a “mineração verde”), são necessárias propostas de aprimoramento. Estas incluem a harmonização do regime tributário de IRPF, eliminando a distorção *onshore/offshore*, e a modernização efetiva dos registros empresariais (DREI) e imobiliários, para que possam recepcionar e conferir publicidade a atos estruturados em *smart contracts* e tecnologia DLT. Sem essa segurança jurídica e simplificação fiscal, a inovação brasileira permanecerá aquém de seu potencial, operando em modelos híbridos ou sendo suplantada por jurisdições com regulação mais clara e eficiente.

REFERÊNCIAS

ASQUINI, Alberto. Profili dell'impresa. **Rivista Commerciale**, [s. l.], v. 41, 1943.

BRASIL. **Lei nº 5.172, de 25 de outubro de 1966**. Dispõe sobre o Sistema Tributário Nacional e institui normas gerais de direito tributário aplicáveis à União, Estados e Municípios. Diário Oficial da União, Brasília, DF, 27 out. 1966.

BRASIL. **Lei nº 6.385, de 7 de dezembro de 1976**. Dispõe sobre o mercado de valores mobiliários e cria a Comissão de Valores Mobiliários. Diário Oficial da União, Brasília, DF, 9 dez. 1976.

BRASIL. **Lei nº 6.404, de 15 de dezembro de 1976**. Dispõe sobre as Sociedades por Ações. Diário Oficial da União, Brasília, DF, 17 dez. 1976.

BRASIL. **Lei nº 8.934, de 18 de novembro de 1994**. Dispõe sobre o Registro Público de Empresas Mercantis e Atividades Afins e dá outras providências. Diário Oficial da União, Brasília, DF, 21 nov. 1994.

BRASIL. **Lei nº 8.981, de 20 de janeiro de 1995**. Altera a legislação tributária federal e dá outras providências. Diário Oficial da União, Brasília, DF, 23 jan. 1995.

BRASIL. **Lei nº 9.250, de 26 de dezembro de 1995**. Altera a legislação do imposto de renda das pessoas físicas e dá outras providências. Diário Oficial da União, Brasília, DF, 27 dez. 1995.

BRASIL. **Lei nº 9.613, de 3 de março de 1998**. Dispõe sobre os crimes de “lavagem” ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; cria o Conselho de Controle de Atividades Financeiras - COAF, e dá outras providências. Diário Oficial da União, Brasília, DF, 4 mar. 1998.

BRASIL. **Medida Provisória nº 2.200-2, de 24 de agosto de 2001.** Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências. Diário Oficial da União, Brasília, DF, 27 ago. 2001.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002.** Institui o Código Civil. Diário Oficial da União: seção 1, Brasília, DF, ano 139, n. 8, p. 1-74, 11 jan. 2002.

BRASIL. **Lei nº 13.874, de 20 de setembro de 2019.** Institui a Declaração de Direitos de Liberdade Econômica [...]. Diário Oficial da União. seção 1, Brasília, DF, ano 150, p. 1-4, 20 set 2019.

BRASIL. **Lei nº 14.478, de 21 de dezembro de 2022.** Dispõe sobre diretrizes a serem observadas na prestação de serviços de ativos virtuais [...]. Diário Oficial da União, Brasília, DF, 22 dez. 2022.

BRASIL. **Lei nº 14.754, de 12 de dezembro de 2023.** Dispõe sobre a tributação de aplicações em fundos de investimento no País e da renda auferida por pessoas físicas residentes no País em aplicações financeiras, entidades controladas e trusts no exterior [...]. Diário Oficial da União, Brasília, DF, 13 dez. 2023.

BRASIL. Departamento Nacional de Registro Empresarial e Integração (DREI). **Instrução Normativa DREI nº 81, de 10 de junho de 2020.** Dispõe sobre as normas e diretrizes gerais do Registro Público de Empresas [...]. Diário Oficial da União, Brasília, DF, 15 jun. 2020.

BRASIL. Departamento Nacional de Registro Empresarial e Integração (DREI). **Ofício Circular SEI nº 4081/2020/ME,** de 1º de dezembro de 2020. Assunto: Integralização de capital social com criptomoedas.

BRASIL. Receita Federal do Brasil (RFB). **Instrução Normativa RFB nº 1.888, de 3 de maio de 2019.** Institui e disciplina a obrigatoriedade de prestação de informações relativas às operações realizadas com

criptoativos à Secretaria Especial da Receita Federal do Brasil (RFB). Publicado(a) no DOU de 07/05/2019, seção 1, página 14.

BRASIL. Receita Federal do Brasil (RFB). **Perguntas e Respostas IRPF 2022**. Disponível em: <https://www.gov.br/receitafederal/pt-br/centrais-de-conteudo/publicacoes/perguntas-e-respostas/dirpf/pr-irpf-2022.pdf/view>. Acesso em: 8 jan. 2025.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial: REsp 1495920**. Relator: Tarso Sanseverino. DJ: 07/06/2018. 2018. Disponível em: https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ATC&sequencial=78697795&num_registro=201402953009&data=20180607&tipo=5&formato=PDF. Acesso em: 15 jan. 2024.

CARVALHO, Alexey. Tecnologia, Informação e Competitividade Empresarial. **Recortes de Gestão**, p. 127-136, 2014.

CASINO, Fran; DASAKLIS, Thomas; PATSAKIS, Constantinos. A systematic literature review of blockchain-based applications: Current status, classification and open issues. **Telematics and Informatics**, v. 36, 2018, p. 55-81.

CAVALCANTI, Mariana Oliveira de Melo; NÓBREGA, Marcos. Smart contracts ou “contratos inteligentes”: o direito na era da blockchain. **Revista Científica Disruptiva**, CERS, v. II, n. 1, 2020, p. 91-118.

COELHO, Fábio Ulhoa. **Manual de Direito Comercial: Direito de Empresa**. 33. ed. rev. atual. e aum. São Paulo: Revista dos Tribunais, 2022.

COMISSÃO DE VALORES MOBILIÁRIOS (CVM). **Parecer de Orientação CVM nº 40**, de 11 de outubro de 2022. Dispõe sobre os criptoativos que são valores mobiliários.

COSTA, Isac. Enfim, as regras do Banco Central sobre ativos virtuais. **ConJur**, 12 nov. 2025. Disponível em: <https://www.conjur.com.br/2025-nov-12/enfim-as-regras-do-banco-central-sobre-ativos-virtuais/>. Acesso em: 15 nov. 2025.

COSTA, Isac Silveira da. O futuro é infungível: tokenização, non-fungible tokens (NFTs) e novos desafios na aplicação do conceito de valor mobiliário. **Revista de Direito das Sociedades e dos Valores Mobiliários**, v. Especial, p. 283-323, 2021.

COSTA, Isac Silveira da. O longo caminho antes do primeiro passo: os projetos de lei sobre ativos virtuais no Brasil. In: FERNANDES, Andressa Guimarães Torquato; CARVALHO, André Castro. **Manual de Criptoativos**. São Paulo: Almedina, 2022.

COSTA, Isac Silveira da. Plunct, plact, zum: Tokens, valores mobiliários e a CVM. In: MOSQUERA, Roberto Quiroga; PINTO, Alexandre Evaristo; EROLES, Pedro. **Criptoativos: estudos jurídicos, regulatórios e tributários**. São Paulo: Quartier Latin, 2021.

FONSECA, Julianna Ramalho. **Tecnologia Blockchain e Smart Contracts sob a Ótica do Direito Empresarial: aspectos contratuais e societários**. Avaliação semestral (Pós-Graduação *lato sensu* em Direito Digital). Rio de Janeiro: ITS Rio/UERJ/CEPED, 2024.

FORGIONI, Paula A. **Contratos Empresariais: Teoria Geral e Aplicação**. 3. ed. rev. atual. e aum. São Paulo: Revista dos Tribunais, 2016.

FRIEDMAN, Milton. The Quantity Theory of Money: A Restatement. In: **Studies in the Quantity Theory of Money**. Chicago: University of Chicago Press, 1956. p. 3-21.

GAGLIANO, Pablo Stolze; PAMPLONA FILHO, Rodolfo. **Manual de Direito Civil**. 4. ed. rev. atual. e aum. São Paulo: SaraivaJur, 2020.

HOFFERT, Antonio. **Criptonomia**: Dos primórdios do dinheiro à Economia pós-blockchain. [S. l.: s. n.], 2019.

LEITE, Luiza; SCHWARTZ, Rodrigo; FEIGELSON, Bruno (coord.). **Tax 4.0**: tributação na realidade exponencial. São Paulo: Thomson Reuters, 2021.

LOBO, Paulo. **Direito Civil**: Contratos. 1. ed. São Paulo: Saraiva, 2011.

LUIZ, Edson. **Do Escambo à inclusão financeira**. Rio de Janeiro: Linotipo Digital, 2014.

MACHADO SEGUNDO, Hugo de Brito. **Tributação e novas tecnologias**: software - criptomoedas - disponibilização de conteúdo - inteligência artificial. Indaiatuba: Editora Foco, 2020.

MAMEDE, Gladston. **Direito Societário**: Direito Empresarial Brasileiro. 4. ed. rev. e atual. São Paulo: Grupo GEN (Editora Atlas), 2022.

MIGALHAS. Ministro Bellizze explica desafios de se regular contratos digitais. **Migalhas**, 27 jun. 2023. Disponível em: <https://www.migalhas.com.br/quentes/388978/ministro-bellizze-explica-desafios-de-se-regular-contratos-digitais>. Acesso em: 10 jan. 2024.

NAKAMOTO, Satoshi. **Bitcoin**: A Peer-to-Peer Electronic Cash System. 2008. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 10 nov. 2025.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). **The Tokenisation of Assets and Potential Implications for Financial Markets**. OECD Blockchain Policy Series. Paris, 2020.

PISCITELLI, Tathiane; SILVEIRA, Daniela (coord.). **Tributação da economia digital**. São Paulo: Thomson Reuters, 2022.

PORTO, Antônio Maristrello; LIMA JUNIOR, João Manoel de; SILVA, Gabriela Borges. Tecnologia Blockchain e direito societário: aplicações práticas e desafios para a regulação. **Revista de Informação Legislativa – RIL**, Brasília, DF, v. 56, n. 223, p. 11-30, jul./set. 2019.

RAMOS, André Luiz Santa Cruz. **Direito empresarial**: volume único. 10. ed. Rio de Janeiro: Forense; São Paulo: MÉTODO, 2020.

SACRAMONE, Marcelo Barbosa. **Manual de Direito Empresarial**. 3. ed. São Paulo: SaraivaJur, 2022.

SANAS, Caio Fernando. **O Futuro dos Contratos**: potencialidades e desafios dos smart contracts no Brasil. 1. Ed. Volta Redonda, Rio de Janeiro: Editora Jurimestre, 2021.

SATO, Renato Cesar. Prefácio. *In*: SANAS, Caio Fernando. **O Futuro dos Contratos**: potencialidades e desafios dos smart contracts no Brasil. 1. Ed. Volta Redonda, Rio de Janeiro: Editora Jurimestre, 2021. p. 15-16.

SCHECHTMAN, David Casz. Introdução a smart contracts. **Revista de Direito e as Novas Tecnologias**, v. 5, 2019, p. 10-25.

SZABO, Nick. Smart Contracts: Formalizing and Securing Relationships on Public Networks. **First Monday**, v. 2, n. 9, 1997. Disponível em: <https://firstmonday.org/ojs/index.php/fm/article/view/548>. Acesso em: 11 jul. 2024.

TAPSCOTT, Don; TAPSCOTT, Alex. **Blockchain Revolution**: como a tecnologia por trás do Bitcoin está mudando o dinheiro, os negócios e o mundo. Tradução: Antonio Carlos Pasquale de Souza Amorim et al. São Paulo: SENAI-SP Editora, 2016.

TARTUCE, Flávio. **Direito Civil**: Teoria Geral dos Contratos e Contratos em espécie. 16. ed. rev. atual. e aum. São Paulo: Grupo GEN (Editora Forense), 2021. v. 3.

TEIXEIRA, Tarcisio. **Direito empresarial sistematizado**: doutrina, jurisprudência e prática. 7. ed. São Paulo: SaraivaJur, 2018.

UHDRE, Dayana de Carvalho. Tokenização, consumo de intangíveis e responsabilização das plataformas digitais: um novo (velho) problema? **Revista Jurídica da Procuradoria-Geral do Estado do Paraná**, Curitiba, n.º 14, p. 11-39, 2023.

6. A TOKENIZAÇÃO DE ATIVOS COMO INSTRUMENTO DE DEMOCRATIZAÇÃO DO ACESSO AOS INVESTIMENTOS NO MERCADO DE CAPITAIS BRASILEIRO

Matheus Silva Reis

Especialista em Direito Digital pelo Instituto de Tecnologia e Sociedade do Rio de Janeiro – ITS Rio em parceria com o Centro de Estudos e Pesquisas no Ensino do Direito da Universidade do Estado do Rio de Janeiro (CEPED/ UERJ).

1. INTRODUÇÃO

Diante das profundas transformações observadas no mercado financeiro nos últimos anos, impulsionadas, entre outros fatores, pela inserção dos criptoativos à economia global, tem-se verificado o surgimento de novos modelos de negócios, instrumentos financeiros e estruturas operacionais que desafiam os paradigmas tradicionais do mercado de capitais, impondo a necessidade de mecanismos de adaptação a essa nova estrutura do mercado.

A infraestrutura dos criptoativos se caracteriza por um elevado grau de participação dos agentes envolvidos, estimulando condutas cooperativas por meio de mecanismos contínuos de incentivo, orientados à sustentabilidade e ao funcionamento eficiente da rede. Sob essa ótica, a dinâmica colaborativa fomenta a inovação tecnológica e a flexibilização das estruturas tradicionais de propriedade, ampliando o uso de mecanismos de troca interpessoal e fortalecendo as interações econômicas entre os indivíduos¹²².

A consolidação de ecossistemas digitais voltados à integração e ao fortalecimento da sociedade em rede tem impulsionado o

122 MATOS, Daniel Oliveira. Aspectos econômicos dos criptotativos e a valoração de preço com base no fluxo de dados. *In*: Daniel de Paiva Gomes; Eduardo de Paiva Gomes; Paulo Cesar Conrado, em coordenação. **Criptoativos, Tokenização, Blockchain e Metaverso: aspectos filosóficos, tecnológicos, jurídicos e econômicos**. São Paulo: Thomson Reuters Brasil, 2022. p. 363-364.

surgimento de modelos de negócios estruturados na lógica da economia compartilhada, uma vez que a ampla e quase irrestrita circulação de informações favorece iniciativas que promovem a distribuição descentralizada de recursos¹²³.

A economia *peer-to-peer* (P2P)¹²⁴ constitui um modelo amplo fundamentado na oferta de produtos e serviços mediados por tecnologias de informação e comunicação e voltados ao consumo coletivo. Ao favorecer interações colaborativas e descentralizadas, a economia P2P promove maior eficiência, amplia o acesso a oportunidades econômicas e reforça a integração da sociedade em rede, que se reflete em seu crescimento expressivo, com projeção de valor superior a USD 1.380,80 bilhões até 2034, partindo de cerca de USD 176,5 bilhões em 2025¹²⁵.

A intensificação da implementação da tecnologia de registro distribuído (*Distributed Ledger Technology DLT*), com destaque para *blockchain*, tem sido apontada como um dos vetores mais significativos de inovação no âmbito dos mercados financeiros e de capitais, ao oferecer novas formas de estruturar, registrar e liquidar transações de forma mais eficiente, transparente e descentralizada. Entre suas aplicações, se destaca a emissão de instrumentos, custódia, liquidação

123 CHEN, Yihan. *The sharing economy: analyses and perspectives from an economic perspective*. International Journal of Information Management, v. 43, p. 328-341, 2018. Disponível em: <https://doi.org/10.1016/j.ijinfomgt.2018.07.004>. Acesso em: 15 de janeiro de 2026.

124 Juho Hamari, Mimmi Sjöklint e Antti Ukkonen definem a economia compartilhada como “an umbrella concept that encompasses several ICT developments and technologies, among others CC, which endorses sharing the of goods and services through online platforms” (HAMARI, Juho; SJÖKLINT, Mimmi; UKKONEN, Antti. The Sharing Economy: Why People Participate in Collaborative Consumption. Journal of the Association for Information Science and Technology, v. 67, p. 2047-2059, Set 2016, DOI 10.1002/asi.23552, ISSN 2330-1643. Disponível em: <https://www.researchgate.net/publication/255698095>. Acesso em: 15 de janeiro de 2026.

125 PRECEDENCE RESEARCH. *PeertoPeer (P2P) lending market size to exceed USD 1,380.80 billion by 2034 driven by digitalization and fintech adoption*. Globe Newswire, 05 set. 2025. Disponível em: <https://www.globenewswire.com/news-release/2025/09/05/3145304/0/en/Peer-to-Peer-P2P-Lending-Market-Size-to-Exceed-USD-1-380-80-Billion-by-2034-Driven-by-Digitalization-and-Fintech-Adoption.html> . Acesso em: 15 de janeiro de 2026.

e negociação de valores mobiliários, com potencial de reduzir custos, aumentar a confiança e ampliar o acesso aos investidores¹²⁶.

A economia digital, que atualmente representa cerca de 15 % do Produto Interno Bruto global, equivalente a aproximadamente US\$ 16 trilhões em 2024¹²⁷, tem se consolidado como um vetor central de transformação econômica ao permitir a alocação de recursos, em sua maioria ociosos, em resposta à demanda coletiva. Dessa forma, viabiliza a inclusão de indivíduos com menor poder aquisitivo no mercado de capitais, tradicionalmente restrito a grandes investidores e a indivíduos de alta renda, promovendo maior democratização do acesso a instrumentos financeiros e fomentando a participação econômica mais ampla da sociedade.

O processo de tokenização consiste na transformação de ativos “físicos” em ativos digitais, sendo utilizada a tecnologia blockchain/ DLT, a qual se caracteriza como uma tecnologia de armazenamento e edição compartilhada de dados¹²⁸.

Com investimentos adequados na tokenização de ativos voltados ao mercado financeiro, projeta-se que a capitalização de mercado desses ativos poderá atingir aproximadamente US\$ 2 trilhões até 2030, podendo alcançar cenários próximos de US\$ 4 trilhões¹²⁹, evidenciando o considerável potencial transformador dessa tecnologia, tanto para a

126 GFMA; BOSTON CONSULTING GROUP; ASHURST; SULLIVAN & CROMWELL. *The Impact of DLT in Capital Markets: Ready for Adoption, Time to Act*. Joint Trades Report, 19 Aug. 2025. Disponível em: <https://www.gfma.org/policies-resources/joint-trades-publish-report-on-the-impact-of-dlt-in-capital-markets/>. Acesso em: 15 de janeiro de 2026.

127 GLOBAL DIGITAL ECONOMY REPORT 2025. *The digital economy comprises about 15 % of world GDP and accounts for approximately USD 16 trillion in 2024*. IDCA, 2025. Disponível em: <https://www.idca.org/insights/qUi9XgvyrzSkyDUy9Tqr>. Acesso em: 15 de janeiro de 2026.

128 ANBIMA. Tokenização de ativos. Disponível em: <https://www.anbima.com.br/data/files/02/30/82/CB/68001810C27A8F08882BA2A8/Tokenizacao%20de%20ativos.pdf>. Acesso em: 15 de janeiro de 2026.

129 MCKINSEY & COMPANY. *Tokenized financial assets: From pilot to scale — The transformational power of tokenizing assets*. McKinsey & Company, 2024. Disponível em: <https://www.mckinsey.com.br/en/industries/financial-services/our-insights/from-ripples-to-waves-the-transformational-power-of-tokenizing-assets>. Acesso em: 15 de janeiro de 2026.

melhoria da eficiência de mercado quanto para a mitigação de riscos nos sistemas financeiros globais.

O presente trabalho tem como objetivo apresentar uma visão geral da conjuntura da tokenização e do mercado de capitais brasileiro, a partir de uma perspectiva multifacetada da tokenização e da tecnologia blockchain, bem como analisar a regulamentação vigente aplicável à temática.

2. TOKENIZAÇÃO DE ATIVOS: CONCEITOS, CARACTERÍSTICAS E FUNDAMENTOS TECNOLÓGICOS.

2.1 Conceito tokenização de ativos

A tokenização consiste pelo conjunto de procedimentos destinados à conversão de direitos sobre um ativo em *tokens* digitais registradas em uma *blockchain* ou em plataforma de tecnologia de registro distribuído (DLT)¹³⁰.

Este método conecta ativos do mundo real (RWA, na sigla em inglês) a um *token* em uma DLT, usando contratos inteligentes (*smart contracts*) para automatizar a gestão, transferência e execução de transações atômicas de Entrega contra Pagamento (DvP), além de permitir a incorporação de regras de supervisão, monitoramento e autorregulação¹³¹.

Logo, esse vínculo transcende uma mera conectividade sistemática e tecnológica, se configurando como uma relação de natureza jurídica, fundamental para a efetividade do processo de tokenização, visto que estabelece a base sobre a qual são atribuídos direitos e obrigações aos detentores do *token* em relação ao ativo subjacente, podendo apresentar características, formas e

130 OCDE. *The tokenisation of assets and potential implications for financial markets*. OECD Blockchain Policy Series, 2020.

131 B3. Tokenização de ativos: o que é, como funciona e quais seus benefícios. Disponível em: <<https://borainvestir.b3.com.br/tipos-de-investimentos/renda-variavel/criptoativos/tokenizacao-de-ativos-o-que-e-como-funciona-e-quais-seus-beneficios/>>. Acesso em: 15 de janeiro de 2026.

procedimentos específicos, regidos pelos instrumentos contratuais ou programáticos que regem a operação. Sua definição exata é, portanto, essencial para garantir segurança jurídica, transparência e funcionalidade ao processo de tokenização.

Em síntese, após um ativo ser tokenizado, o detentor ou portador do *token* resultante é investido, em certa medida, em certa medida e conforme o regramento jurídico, nos direitos e obrigações que possuiria caso fosse o detentor direto do objeto ou ativo do mundo real ao qual o vínculo foi estabelecido – o objeto ou ativo tokenizado.

3. BLOCKCHAIN E SMART CONTRACTS COMO INFRAESTRUTURA TECNOLÓGICA

A *blockchain*, uma cadeia de blocos digitais que armazena informações, é um sistema de DLT que alcança consenso em uma rede descentralizada, registrando dados de forma confiável e imutável, aumentando a segurança e a transparência em transações e interações digitais¹³².

Cada bloco é composto por 3 fatores: informação; *hash* (espécie de código de identificação única, semelhante a uma impressão digital) e o *hash of previous block* (código do bloco anterior). Essa estrutura cria uma cadeia de blocos interligados, garantindo transparência e segurança ao sistema, já que qualquer alteração no conteúdo de um bloco modifica automaticamente seu *hash*¹³³.

O marco decisivo de instituição da *blockchain* ocorreu em 2008, com a divulgação do *whitepaper* do Bitcoin, publicado sob o pseudônimo Satoshi Nakamoto, que popularizou a *blockchain*, como um sistema capaz de registrar transações de forma distribuída,

132 KIKTENKO, EO. et al. *Quantum-secured blockchain*. Quantum Science and Technology, IOP Publishing, v. 3, n. 3, p. 8, 2018.

133 ROVAI, Armando Luiz; SILVA, André Luis Caetano. Possibilidade jurídica de integralização do capital social através de criptomoeda e ativos similares. In: Alexandre Evaristo Pinto; Pedro Eroles; Roberto Quiroga Mosquera, em coordenação. *Criptoativos – Estudo Regulatórios e Tributários*. São Paulo: Quartier Latin, 2021. p. 531-533.

transparente e imutável, além de introduzir o Bitcoin ao mercado financeiro, apresentando a ideia de uma moeda digital descentralizada e de um mecanismo de criptomoeda ponto a ponto, sem necessidade de intermediários¹³⁴.

Os contratos inteligentes (*smart contracts*) na *blockchain* são autoexecutáveis, definidos por consenso, e asseguram a governança de tokens, além de garantir segurança e confiabilidade nas transações.¹³⁵. As DLTs incorporaram o princípio de escassez para bens digitais, em dissonância com a facilidade de reprodução típica desses ativos, de modo que tal escassez garante a singularidade e possibilidade de verificação de cada registro.

A utilização das DLTs evidencia seu amplo potencial para facilitar e regulamentar transações envolvendo tanto ativos quanto direitos do mundo real, promovendo maior valorização e acessibilidade desses ativos por meio de sua integração tecnológica.

4. TIPOS DE ATIVOS TOKENIZADOS

Um *token* é, essencialmente, uma representação digital de um ativo, direito ou utilidade registrada em uma *blockchain*.

No mundo da criptoeconomia, os *tokens* ou criptoativos podem ser classificados segundo sua função, natureza jurídica, estrutura, tipo de rede *blockchain* empregada, entre outros critérios de categorização. Os *tokens* mantêm sua definição e propósito fundamentais, mas com segurança criptográfica adicional para prova e auditabilidade.

Em linhas gerais, os *tokens* se distinguem em *tokens* fungíveis e não fungíveis: os primeiros são intercambiáveis entre si e possuem valor equivalente, sendo amplamente utilizados como instrumentos de troca, liquidez e circulação de valor, enquanto os tokens não fungíveis

134 NAKAMOTO, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 15 de janeiro de 2026.

135 HU, Yining; LIYANAGE, Madhusanka; MANSOOR, Ahsan; THILAKARATHNA, Kanchana; JOURJON, Guillaume; SENEVIRATNE, Aruna. *Blockchain-based Smart Contracts - Applications and Challenges*. Disponível em: <https://arxiv.org/abs/1810.04699>. Acesso em: 15 de janeiro de 2026.

(NFTs) são únicos, indivisíveis e dotados de identidade própria, o que os torna adequados para a representação de ativos singulares, como obras de arte, colecionáveis, certificados e determinados bens físicos ou digitais. Além dessa distinção, os *tokens* também podem ser classificados de acordo com sua função econômica, se destacando os *utility tokens*, destinados a conceder acesso a produtos, serviços ou funcionalidades específicas dentro de um ecossistema digital; os *security tokens*, que representam valores mobiliários e conferem direitos econômicos ou societários, como participação nos lucros, rendimentos ou direito de voto, estando sujeitos à regulação do mercado de capitais; e os *payment tokens*, cuja finalidade principal é atuar como meio de pagamento descentralizado, permitindo transferências de valor de forma rápida, segura e sem intermediários¹³⁶.

A definição legal e regulamentar de criptoativos e *tokens* exerce papel central nos mercados em que atuam, produzindo efeitos jurídicos e regulatórios relevantes. Uma conceituação excessivamente restrita pode reduzir o alcance do regime jurídico aplicável, ao passo que uma abordagem demasiadamente ampla pode sujeitar à regulação de ativos que, em princípio, não demandariam supervisão normativa.

De forma abrangente, os *tokens* possuem potencial para se consolidarem como o alicerce da nova economia digital. Neste trabalho, adotaremos a definição de *tokens* apresentada no Parecer de Orientação nº 40/2022 da Comissão de Valores Mobiliários (CVM)¹³⁷, os quais são organizados em três categorias distintas, cada uma com aplicações específicas:

(i) Token de Pagamento (cryptocurrency ou payment token):

busca replicar as funções de moeda, notadamente de unidade de conta, meio de troca e reserva de valor;

136 GUERREIRO, José Alexandre Tavares; BUSCHINELLI, Gabriel Saad Kik. ICOs (Initial Coin Offerings) e a Disciplina dos Valores Mobiliários. In: Alexandre Evaristo Pinto; Pedro Eroles; Roberto Quiroga Mosquera, em coordenação. **Criptoativos – Estudo Regulatórios e Tributários**. São Paulo: Quartier Latin, 2021. p. 467-486.

137 COMISSÃO DE VALORES MOBILIÁRIOS (CVM). *Parecer de Orientação CVM nº 40, de 11 de outubro de 2022*. Disponível em: <https://conteudo.cvm.gov.br/legislacao/pareceres-orientacao/pare040.html>. Acesso em: 15 de janeiro de 2026.

(ii) Token de Utilidade (utility token): utilizado para adquirir ou acessar determinados produtos ou serviços; e

(iii) Token referenciado a Ativo (asset-backed token): representa um ou mais ativos, tangíveis ou intangíveis. São exemplos os “security tokens”, as stablecoins, os non-fungible tokens (NFTs) e os demais ativos objeto de operações de “tokenização”.

5. O MERCADO DE CAPITAIS BRASILEIRO: ESTRUTURA E DESAFIOS DE ACESSO AO INVESTIMENTO

5.1. Estrutura do mercado de capitais do Brasil

O mercado de capitais brasileiro possui um protagonismo relevante no cenário econômico nacional, sendo responsável pela mobilização de volumes expressivos de recursos destinados ao financiamento das atividades produtivas, à expansão empresarial e à canalização da poupança privada para investimentos de médio e longo prazo.

Ademais, é de suma importância compreender que a relevância do mercado de capitais não se limita ao montante financeiro transacionado, mas também decorre de seu papel estratégico na diversificação das fontes de financiamento da economia, historicamente concentradas no crédito bancário¹³⁸.

A estrutura do mercado de capitais no Brasil foi construída a partir de um modelo institucional fortemente regulado, com atuação coordenada entre entes estatais e privados, principalmente, pela criação da CVM, com a edição da Lei n.º 6.385/1976¹³⁹, como órgão

138 ANBIMA – ASSOCIAÇÃO BRASILEIRA DAS ENTIDADES DOS MERCADOS FINANCEIRO E DE CAPITAIS. Estudo da ANBIMA mostra contribuição do mercado de capitais para o desenvolvimento econômico brasileiro. Disponível em: <https://www.anbima.com.br/data/files/8E/B4/5C/C7/F26C7910C05C4A79B82BA2A8/A%20contribui%C3%A7%C3%A3o%20do%20mercado%20de%20capitais%20para%20o%20desenvolvimento%20econ%C3%B4mico.pdf>. Acesso em: 15 de janeiro de 2026.

139 BRASIL. Lei n.º 6.385, de 7 de dezembro de 1976. Dispõe sobre o mercado de valores mobiliários e cria a Comissão de Valores Mobiliários. Diário Oficial da União, Brasília,

regulador do mercado de capitais, sucedendo a instituição Conselho Monetário Nacional e Banco Central do Brasil, ambos frutos da edição da Lei n.º 4.595/1964¹⁴⁰. Essa estrutura se baseou em uma política voltada ao desenvolvimento financeiro, visando estimular a formação de poupança e sua alocação para atividades produtivas, por meio de um portfólio diversificado e em expansão de instrumentos de mercado¹⁴¹.

A CVM ocupa posição central como órgão estatal incumbido pela regulação, fiscalização e desenvolvimento do mercado de valores mobiliários, exercendo funções normativas, fiscalizatórias, sancionatórias etc. Sua atuação abrange tanto no mercado primário relativo à emissão de valores mobiliários, quanto no mercado secundário, responsável pela negociação desses ativos, elemento essencial para a liquidez e formação de preços de mercado¹⁴².

Ao lado da regulação estatal, o mercado brasileiro dispõe também de um sofisticado sistema de autorregulação, no qual se destaca a B3, única bolsa de valores em funcionamento no país. Em 2025, o volume médio diário negociado no mercado à vista na B3 alcançou cerca de R\$ 29,05 bilhões, refletindo crescimento anual¹⁴³.

Complementam essa estrutura entidades autorreguladoras e de recomendação, como a Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais (ANBIMA), Associação dos Analistas e Profissionais de Investimentos do Mercado de Capitais (APIMEC)

09 dez. 1976. Disponível em: https://www.planalto.gov.br/ccivil_03/Leis/L6385.htm. Acesso em: 15 de janeiro de 2026.

140 BRASIL. Lei nº 4.595, de 31 de dezembro de 1964. Dispõe sobre a política e o Sistema Financeiro Nacional e cria o Banco Central do Brasil. Diário Oficial da União, Brasília, 31 dez. 1964. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L4595.htm. Acesso em: 15 de janeiro de 2026.

141 YAZBEK, Otávio. Regulação do Mercado Financeiro e de Capitais. Rio de Janeiro: Elsevier. 2007, p. 259.

142 ARAUJO. Danilo Borges dos Santos Gomes de. Regulação Brasileira do Mercado de Capitais. São Paulo: Saraiva, 2015, p. 31.

143 B3. Volume médio diário de negociação no mercado à vista na B3 atinge R\$ 29 bilhões, alta de 3,4 % em 12 meses, revela DataWise+. São Paulo: B3, 12 dez. 2025. Disponível em: https://www.b3.com.br/pt_br/noticias/volume-medio-diario-de-negociacao-no-mercado-a-vista-na-b3-atinge-r-29-bilhoes-alta-de-3-4-em-12-meses-revela-datawise.htm. Acesso em: 15 de janeiro de 2026.

e Associação Nacional das Corretoras e Distribuidores de Títulos Mobiliários, Câmbio e Mercadorias (ANCORD), que contribuem para a padronização de práticas, fiscalização de condutas e elevação dos padrões éticos e fiduciários do mercado.

O resultado é a formação de uma rede regulatória híbrida, composta por entes públicos e privados, que visa garantir o funcionamento eficiente, transparente e estável do mercado de capitais brasileiro, alinhando-o às melhores práticas internacionais e ampliando sua atratividade para investidores nacionais e estrangeiros.

5.2. Barreiras tradicionais ao acesso de investidores

As restrições no acesso de investidores ao mercado de capitais representam um obstáculo estrutural que limita a participação de agentes menos experientes ou com menor capacidade financeira, afetando o desenvolvimento, a profundidade e a liquidez do mercado.

No âmbito da regulação vigente no Brasil, embora se busque proteger o investidor de varejo por meio de critério de adequação e segmentação dos produtos financeiros, tais normas delimitam o acesso entre diferentes categorias de investidores. À título de exemplificação, a criação do investidor qualificado ou profissional pela CVM¹⁴⁴, a qual confere os portfólios específicos, restringindo, assim, a participação de determinados agentes em segmentos de ativos ou estruturas de investimento mais sofisticadas, como fundos exclusivos e instrumentos financeiros no exterior¹⁴⁵.

144 COMISSÃO DE VALORES MOBILIÁRIOS – CVM. Resolução CVM nº 175, de 23 de dezembro de 2022. Dispõe sobre a constituição, o funcionamento e a divulgação de informações dos fundos de investimento, bem como sobre a prestação de serviços para os fundos, e revoga as normas que especifica. Disponível em: <https://conteudo.cvm.gov.br/export/sites/cvm/legislacao/resolucoes/anexos/100/resol175.pdf>. Acesso em: 15 de janeiro de 2026.

145 ASA – Análise CVM. Investidores no mercado de capitais brasileiro. Brasília: CVM, 19 jul. 2021. Disponível em: https://www.gov.br/cvm/pt-br/centrais-de-conteudo/publicacoes/estudos/air_investidores-no-mercado-de-capitais-brasileiro_2021-07-19.pdf. Acesso em: 15 de janeiro de 2026.

A complexidade das normas, aliada à necessidade de maior educação financeira e aos elevados custos de ingresso em mercados específicos, como ofertas públicas iniciais e dívida corporativa, constitui barreiras à ampliação da base de investidores. Pesquisas internacionais indicam que lacunas no conhecimento financeiro figuram entre os principais obstáculos à participação de investidores de varejo, evidenciando a importância de políticas públicas e iniciativas privadas voltadas à promoção da literacia financeira¹⁴⁶.

Esses fatores, aliados a obstáculos burocráticos e regulatórios para pequenas e médias empresas, evidenciam o caráter restritivo de barreiras tradicionais que vão além da proteção do investidor, envolvendo também estrutura e custos de atuação no mercado de valores mobiliários. Superá-las é essencial para democratizar o mercado de capitais, ampliar a participação de investidores e emissores e fortalecer o financiamento de longo prazo.

5.3. Inclusão financeira e democratização dos investimentos

A inclusão financeira e a democratização dos investimentos são essenciais para ampliar a participação de diferentes segmentos da sociedade no mercado de capitais. A inclusão financeira implica não apenas a disponibilidade de produtos e serviços financeiros, mas também sua efetiva utilização por indivíduos e empresas sistematicamente excluídos do mercado, como pequenos investidores e agentes de baixa renda¹⁴⁷.

146 WORLD ECONOMIC FORUM. *New study finds financial education gaps are primary barrier to retail investing in capital markets*. 04 ago. 2022. Disponível em: <https://www.weforum.org/press/2022/08/new-study-finds-financial-education-gaps-are-primary-barrier-to-retail-investing-in-capital-markets/>. Acesso em: 15 de janeiro de 2026.

147 AMORIM, K. A. F. de; LUCENA, G. K. F.; GIRÃO, L. F. de A. P.; QUEIROZ, D. B. de. A influência da educação financeira na inserção dos investidores no mercado de capitais brasileiro: um estudo com discentes da área de negócios. *RACE – Revista de Administração, Contabilidade e Economia*, v. 17, n. 2, p. 567–590, 2018. DOI: 10.18593/race.v17i2.16834. Disponível em: <https://periodicos.unoesc.edu.br/race/article/view/16834>. Acesso em: 15 de janeiro de 2026.

No Brasil, a educação financeira tem papel central na participação do mercado, uma vez que maior conhecimento financeiro aumenta a probabilidade de ingresso e confiança dos investidores, reduzindo barreiras ao acesso.

Adicionalmente, iniciativas institucionais, como as promovidas pela ANBIMA, voltadas à promoção da diversidade e inclusão no mercado de capitais ilustram a crescente consciência de que a expansão da base de investidores e a construção de ambientes de investimento mais inclusivos dependem de esforços coordenados entre reguladores, associações de mercado e agentes privados¹⁴⁸.

6. A TOKENIZAÇÃO DE ATIVOS COMO INSTRUMENTO DE DEMOCRATIZAÇÃO DO ACESSO AOS INVESTIMENTOS

6.1. Redução de custos e fracionamento de ativos

No contexto do mercado de capitais, a tokenização de ativos representa um mecanismo disruptivo apto a reduzir barreiras estruturais relacionadas à emissão, ao registro, à negociação e à liquidação de valores mobiliários. Historicamente, o acesso a portfólios de investimento se mostrou limitado pelos elevados custos de emissão e pela dependência de infraestruturas centralizadas de custódia e liquidação, que envolvem múltiplos intermediários (emissores, coordenadores, custodiantes etc.). Embora tal arquitetura assegure elevada segurança jurídica, ela acarreta custos significativos de estruturação, manutenção e conformidade regulatória.

Contudo, ao utilizar tecnologia de DLT, principalmente por meio da *blockchain*, a tokenização possibilita a reestruturação da cadeia tradicional de intermediação, produzindo impactos diretos

148 ANBIMA – ASSOCIAÇÃO BRASILEIRA DAS ENTIDADES DOS MERCADOS FINANCEIRO E DE CAPITAIS. Relatório de Diversidade ANBIMA 2025. São Paulo: ANBIMA, 2025. Disponível em: https://www.anbima.com.br/data/files/CC/13/FA/04/59DE89100C12BE89B82BA2A8/Relatorio_Diversidade_Anlima_2025.pdf. Acesso em: 15 de janeiro 2026.

sobre os custos operacionais, a eficiência dos processos de liquidação e a ampliação da base de investidores. Desse modo, viabiliza a desintermediação de procedimentos, com a substituição, na maioria das vezes, de tarefas manuais e onerosas por protocolos automatizados, executados via *smart contracts*.

A tokenização, ao registrar a titularidade e as transferências em rede DLT, mediante mecanismos criptográficos de validação, proporcionando a automatização etapas operacionais por meio de *smart contracts*, com a consequente redução de custos administrativos e operacionais associados à escrituração, à reconciliação e à liquidação¹⁴⁹. Adicionalmente, a liquidação pode ocorrer em prazos substancialmente reduzidos, mitigando os riscos de contraparte e diminuindo exigências de capital associadas ao período de compensação, em dinâmica assemelhada à redução do *settlement risk*¹⁵⁰.

Do ponto de vista econômico, a minimização do ciclo de liquidação implica diretamente no custo de capital do emissor e no custo de oportunidade do investidor, sobretudo nos mercados secundários. A possibilidade de liquidação em tempo praticamente imediato diminui a necessidade de garantias e de reservas de provisionamento, promovendo maior eficiência na alocação de recursos.

Outro aspecto central para o mercado de capitais diz respeito ao fracionamento de ativos pela tokenização, como, por exemplo, debêntures, cotas de fundos, cédulas de crédito bancário, ativos imobiliários e participações societárias, em unidades de menor valor nominal, mantendo proporcionalidade econômica dos direitos creditórios ou societários. Consequentemente, essa granularidade favorece o acesso de investidores de varejo a ativos que,

149 IOSCO – International Organization of Securities Commissions. **Tokenization of Financial Assets**. Pub. Doc. 809, 2025. Disponível em: <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD809.pdf>. Acesso em: 20 de janeiro de 2026.

150 OECD – Organisation for Economic Co-operation and Development. **The Tokenisation of Assets and Potential Implications for Financial Markets**. OECD Blockchain Policy Series, Paris: OECD, 2020. Disponível em: <https://www.blockchainwg.eu/wp-content/uploads/2020/03/The-Tokenisation-of-Assets-and-Potential-Implications-for-Financial-Markets.pdf>. Acesso em: 20 de janeiro de 2026.

tradicionalmente, demandavam aportes elevados, tais como ofertas privadas ou instrumentos estruturados¹⁵¹.

No plano regulatório brasileiro, adota abordagem centrada na substância econômica da operação, especialmente após a edição da Resolução CVM nº 88/2022¹⁵², que modernizou o regime de *crowdfunding* de investimento ao ampliar o limite de captação por oferta para até R\$ 15.000.000,00 (quinze milhões de reais) e disciplinar a atuação das plataformas eletrônicas de investimento participativo.

A Resolução CVM nº 88 promoveu a ampliação do limite de captação por oferta, consolidando, ao mesmo tempo, a utilização de plataformas eletrônicas de investimento participativo. Revelou-se essencial para redução de custos operacionais de distribuição por sociedades empresárias de pequeno porte, bem como para a escrituração de valores mobiliários, mediante por meio de maior eficiência tecnológica. Ademais, facilitar o acesso de investidores de varejo a oportunidades de investimento antes restritas, este regime normativo expandiu a base de empresas habilitadas a captar recursos no mercado, contribuindo para a democratização do acesso ao mercado de capitais.

A importância desse instrumento é corroborada pelos dados do Boletim Econômico da CVM, os quais indicam que, no período de janeiro a setembro de 2025, o volume financeiro captado via *crowdfunding* mais que quadruplicou em comparação ao mesmo intervalo do ano anterior, atingindo aproximadamente R\$ 3,1 bilhões¹⁵³.

151 Vitória, G. M., Araújo Neto, M. J. de, Pinto, D. S. A., & Pereira, V. P. (2025). OS IMPACTOS SOCIOECONÔMICOS DAS CRIPTOMOEDAS E DA TECNOLOGIA BLOCKCHAIN NO FUTURO DO BRASIL: DESAFIOS E OPORTUNIDADES. REVISTA FOCO, 18(11), e10668. Disponível em: <https://doi.org/10.54751/revistafoco.v18n11-187>. Acesso em: 20 de janeiro de 2026.

152 BRASIL. Comissão de Valores Mobiliários (CVM). Resolução CVM nº 88, de 27 de abril de 2022. Regulamenta a oferta pública de distribuição de valores mobiliários de emissão de sociedades empresárias de pequeno porte realizada com dispensa de registro por meio de plataforma eletrônica de investimento participativo. Disponível em: <https://conteudo.cvm.gov.br/export/sites/cvm/legislacao/resolucoes/anexos/001/resol088consolid.pdf>. Acesso em: 20 de janeiro de 2026.

153 COMISSÃO DE VALORES MOBILIÁRIOS (CVM). Boletim Econômico – 3º trimestre de 2025: FII, FIDC e *crowdfunding* são destaques no terceiro trimestre de 2025.

Diante do exposto, a redução de custos advinda da tokenização não resulta da supressão de normas regulatórias, mas sim da maior eficiência tecnológica perante as estruturas de mercado. As emissões tokenizadas têm o potencial de simplificar os processos de distribuição, ampliar a transparência por meio da rastreabilidade em tempo real e aprimorar a governança informacional, desde que sejam rigorosamente observados os deveres legais de divulgação e de proteção ao investidor.

A crescente digitalização dos mercados de capitais tem introduzido mecanismos capazes de incrementar a liquidez de ativos tradicionalmente ilíquidos, como participações de *equity* e direitos creditórios estruturados. Nesse contexto, o fracionamento digital surge como instrumento capaz de expandir a base de investidores, reduzir a concentração de risco e atenuar o desconto por iliquidez associado a tais ativos¹⁵⁴.

Sob a ótica sistêmica, a tokenização pode aproximar o mercado de capitais de um modelo mais inclusivo, no qual a barreira de entrada financeira é reduzida sem comprometer a segurança jurídica. Ao permitir emissões com menor valor mínimo de subscrição e maior divisibilidade econômica, promove-se a democratização do acesso ao investimento, alinhando inovação tecnológica e regulação financeira.

6.2. Ampliação do acesso de investidores

A tokenização impacta significativamente sobre três dimensões estruturais do acesso ao mercado de capitais: (i) barreiras financeiras, mediante redução de aportes mínimos; (ii) barreiras operacionais, ao simplificar os processos de emissão, liquidação e custódia, reduzindo

Brasília: CVM, 28 out. 2025. Disponível em: <https://www.gov.br/cvm/pt-br/assuntos/noticias/2025/fii-fidc-e-crowdfunding-sao-destaques-no-terceiro-trimestre-de-2025>. Acesso em: 20 de janeiro de 2026.

154 WORLD ECONOMIC FORUM. **Asset Tokenization in Financial Markets: The Next Generation of Value Exchange**. 21 May 2025. Disponível em: <https://www.weforum.org/publications/asset-tokenization-in-financial-markets-the-next-generation-of-value-exchange/>. Acesso em: 20 de janeiro de 2026.

custos e intermediários; e (iii) barreiras geográficas, dado o potencial de circulação digital em ambientes descentralizados. Essa reconfiguração favorece a ampliação da capilaridade do mercado e a diversificação da base de investidores, podendo resultar em incremento da eficiência alocativa de recursos¹⁵⁵.

Apesar da ampliação quantitativa do acesso ao mercado proporcionado pela tokenização, tal expansão não implica, por si só, em inclusão financeira qualitativa. A efetiva democratização do investimento depende da capacidade do investidor de compreender a natureza jurídica do *token*, os direitos a ele inerente, os riscos tecnológicos (como falhas programacionais *smart contracts* ou vulnerabilidades de segurança), os riscos econômicos (volatilidade e iliquidez) e o enquadramento regulatório da oferta.

Nesse contexto, a educação financeira assume papel central, constituindo condição indispensável para a legitimidade e a segurança da ampliação do acesso ao mercado de capitais. Além disso, a promoção da literacia financeira fortalece a confiança na tokenização, reduz a probabilidade de práticas especulativas inadequadas e assegura que a democratização do acesso não se limite à mera participação quantitativa, mas se concretize de forma qualitativa.

É necessário ressaltar que a ampliação do acesso a produtos financeiros, no contexto da inclusão financeira, deve ser acompanhada de mecanismos adequados de proteção e capacitação informacional, sob risco de induzir fenômenos de sobre-endividamento ou decisões de investimento inadequadas ao perfil de risco do investidor. No ambiente tokenizado, a assimetria informacional tende a se intensificar em virtude da complexidade tecnológica envolvida e da rapidez na circulação informacional. Diante deste cenário, se impõe a necessidade de adoção de padrões rigorosos de divulgação e

155 WORLD ECONOMIC FORUM. **Asset Tokenization in Financial Markets: The Next Generation of Value Exchange**. 21 May 2025. Disponível em: <https://www.weforum.org/publications/asset-tokenization-in-financial-markets-the-next-generation-of-value-exchange/>. Acesso em: 20 de janeiro de 2026.

transparência (*disclosure*) de informações, essenciais para a proteção dos investidores e para a integridade do mercado¹⁵⁶.

O regime regulatório da CVM e de outras normas correlacionadas estabelece deveres de informação, transparência e de verificação de adequação (*suitability*) como fatores essenciais na proteção do investidor e da mitigação de assimetrias informacionais no mercado de capitais. Essa questão do dever informacional ao investidor, exige que os agentes do mercado verifiquem a adequação dos produtos e serviços ao perfil de risco dos investidores, de modo a reduzir o risco de decisões incompatíveis com os objetivos de investimentos e a tolerância ao risco dos investidores.

Em síntese, a tokenização pode operar como vetor de ampliação do acesso ao investimento, mas sua efetiva contribuição para a democratização do mercado depende da articulação entre inovação tecnológica, regulação proporcional e políticas de educação financeira. A inclusão não deve ser compreendida apenas como expansão numérica de investidores, mas como integração consciente e informada ao sistema financeiro, com preservação da integridade do mercado e proteção do investidor.

6.3. Liquidez, transparência e eficiência de mercado

No âmbito dos mercados financeiros digitais, a tokenização de ativos revela influência relevante sobre a liquidez, ao permitir o fracionamento de ativos tipicamente ilíquidos, como ativos imobiliários, direitos creditórios estruturados, participações societárias (*equity*) e obras de artes. Por meio desse processo, os ativos passam a ser representados em *tokens* divisíveis, negociáveis em plataformas especializadas, o que amplia a acessibilidade e potencializa a circulação no mercado secundário.

156 OECD – Organisation for Economic Co-operation and Development. **The Tokenisation of Assets and Potential Implications for Financial Markets.** OECD Blockchain Policy Series, Paris: OECD, 2020. Disponível em: <https://www.blockchainwg.eu/wp-content/uploads/2020/03/The-Tokenisation-of-Assets-and-Potential-Implications-for-Financial-Markets.pdf>. Acesso em: 20 de janeiro de 2026.

O fracionamento expande a base de potenciais investidores, reduzindo o *ticket* mínimo de participação e facilita a circulação do ativo em mercados secundários. Em termos econômicos, a maior liquidez tende a reduzir o desconto aplicado a ativos ilíquidos, aumentando sua atratividade e potencialmente seu valor de mercado¹⁵⁷.

Agovernança e a transparência são potencializadas pela tecnologia de registro distribuído (DLT), que permite que as transações sejam registradas de forma imutável, rastreável e auditável. A integridade das informações, assegurada por mecanismos criptográficos, contribui para a redução de assimetrias informacionais e mitigação de riscos de manipulação. Os *smart contracts* possibilitam a automação de obrigações contratuais, como pagamento de rendimentos ou distribuição de dividendos, promovendo maior previsibilidade e segurança jurídica das operações.

A eficiência de mercado é aprimorada pela tokenização, que possibilita desintermediação parcial de determinadas operações e a redução decorrente de custos transacionais. Processos tradicionalmente burocráticos, como registro, liquidação e custódia, podem ser integrados e executados de forma quase instantânea na própria rede *blockchain*. A uniformização tecnológica propicia a interoperabilidade entre plataformas e fortalece a concorrência entre intermediários, assegurando o aprimoramento da eficiência sistêmica e da alocação de recursos no mercado de capitais.

Os benefícios decorrentes da tokenização e da inovação financeira dependem de um ambiente regulatório claro e de governança adequada para as plataformas de negociação. A insuficiência de supervisão regulatória pode comprometer a confiança no sistema, ao passo que uma regulamentação excessivamente rígida tende a neutralizar os efeitos positivos da tokenização.

Diante disso, a consolidação da tokenização como instrumento de democratização do acesso a investimentos requer a harmonização

157 MAFRUR, Rischian. **Tokenize Everything, But Can You Sell It? RWA Liquidity Challenges and the Road Ahead**. arXiv, 03 ago. 2025. Disponível em: <https://arxiv.org/abs/2508.11651>. Acesso em: 20 de janeiro de 2026.

entre a inovação tecnológica, segurança jurídica e proteção ao investidor.

7. ASPECTOS REGULATÓRIOS DA TOKENIZAÇÃO DE ATIVOS NO BRASIL

A tokenização de ativos no Brasil se insere em um ambiente regulatório multifacetado, que demanda a atuação coordenada de diferentes autoridades, especialmente a CVM e o Banco Central do Brasil (BCB). A definição do regime jurídico aplicável depende, essencialmente, da natureza do ativo subjacente ao *token* e da estrutura da oferta realizada ao público, o que exige análise casuística à luz do ordenamento vigente.

O Parecer de Orientação nº 40/2022¹⁵⁸ da CVM estabeleceu diretrizes para delimitar a atuação da autarquia na regulação e supervisão de criptoativos no mercado de capitais. O documento adota critério funcional de classificação, distinguindo, em linhas gerais, três categorias de tokens, conforme indicado no item seção 2.3. Em regra, a CVM não enquadra *tokens* de pagamento e *tokens* de utilidade na classificação jurídica de valores mobiliários.

Não obstante, os *tokens* referenciados a ativos podem ser enquadrados como valores mobiliários, a depender da essência econômica dos direitos conferidos aos titulares e da função desempenhada no mercado. A CVM se posiciona no sentido de que que a tecnologia empregada na operação de tokenização (como *blockchain* e *smart contracts*) não constitui o objeto primário de análise regulatória, figurando como elemento acessório no exame da operação. A natureza jurídica do *token* decorre, portanto, das características do ativo subjacente e da estrutura jurídico-econômica da operação.

A tokenização, isoladamente considerada, não depende de registro ou autorização prévia da CVM. Contudo, se o ativo tokenizado

158 COMISSÃO DE VALORES MOBILIÁRIOS (CVM). Parecer de Orientação CVM nº 40, de 11 de outubro de 2022. Disponível em: <https://conteudo.cvm.gov.br/legislacao/pareceres-orientacao/pare040.html>. Acesso em: 20 de janeiro de 2026.

configurar valor mobiliário destinado à distribuição pública, tanto o emissor quanto a oferta estarão sujeitos à regulamentação aplicável.

Para que um criptoativo seja considerado um valor mobiliário e esteja sob a competência da CVM, é necessário que ele represente digitalmente um dos valores mobiliários especificados nos artigos I a VIII da Lei nº 6.385/1976, e/ou na Lei nº 14.430/2022¹⁵⁹, que regulamenta os certificados de recebíveis gerais, ou que se enquadre no conceito amplo de valor mobiliário definido no inciso IX do artigo 2º da Lei nº 6.385.

A caracterização de um ativo como valor mobiliário pelo conceito aberto da norma exige que a CVM analise cada caso de forma concreta. Segundo o teste de Howey¹⁶⁰, são necessários os seguintes critérios: (i) oferta pública para captar recursos; (ii) investimento de recursos avaliáveis; (iii) esforço de terceiros para o sucesso do negócio; (iv) expectativa de retorno econômico; (v) caráter coletivo do investimento; e (vi) existência de instrumento formalizando o negócio.

No âmbito do sistema financeiro, a Lei nº 14.478/2022¹⁶¹ definiu as diretrizes para a prestação de serviços de ativos virtuais e atribuiu ao Poder Executivo a competência para designar a autoridade responsável por sua regulação, incumbência posteriormente conferida ao BCB pelo Decreto nº 11.563/2023¹⁶². Compete ao BCB regular, autorizar e

159 BRASIL. Lei nº 14.430, de 3 de agosto de 2022. Dispõe sobre o Certificado de Recebíveis do Agronegócio (CRA) e o Certificado de Recebíveis Imobiliários (CRI), institui o Certificado de Recebíveis Gerais e altera as Leis nº 8.668, de 25 de junho de 1993, nº 9.514, de 20 de novembro de 1997, e nº 10.931, de 2 de agosto de 2004. 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2022-2026/2022/lei/L14430.htm. Acesso em: 20 de janeiro de 2026.

160 Tem como base um precedente da Suprema Corte dos Estados Unidos, do qual se extrai o “Teste de Howey”, utilizado pela CVM para avaliar se um determinado ativo constitui valor mobiliário. SUPREMA CORTE DOS ESTADOS UNIDOS. SEC v. WJ Howey Co., 328 US 293, 1946.

161 BRASIL. Lei nº 14.478, de 21 de dezembro de 2022. Dispõe sobre diretrizes para a prestação de serviços relacionados a criptoativos no Brasil. 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2022-2026/2022/lei/L14478.htm. Acesso em: 20 de janeiro de 2026.

162 BRASIL. Decreto nº 11.563, de 13 de junho de 2023. Regulamenta a Lei nº 14.478, de 21 de dezembro de 2022, que dispõe sobre diretrizes para a prestação de serviços relacionados a criptoativos. 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11563.htm. Acesso em: 20 de janeiro de 2026.

fiscalizar os prestadores de serviços de ativos virtuais, especialmente quando a atividade envolver intermediação, custódia ou administração de criptoativos.

Até a edição de regulamentação específica da Lei nº 14.478/2022, não se exige licença específica para emissão e distribuição de *tokens*, ressalvada a hipótese de sua caracterização como valores mobiliários, caso em que incidira o regime jurídico aplicável ao mercado de capitais.

A tokenização de ativos suscita reflexões sobre a necessidade de adaptação de institutos tradicionais do direito societário e do mercado de capitais, como escrituração, custódia e registro de valores mobiliários. A legislação brasileira admite a escrituração eletrônica e o registro centralizado, o que abre espaço para integração com tecnologias baseadas em *blockchain*, desde que preservados os requisitos de segurança, rastreabilidade e integridade das informações.

Vale destacar que iniciativas do BCB relacionadas ao desenvolvimento do real digital (Drex) indicam tendência de integração entre tecnologia de registro distribuído e sistema financeiro tradicional, o que pode facilitar a interoperabilidade com ativos tokenizados e ampliar sua adoção institucional.

A perspectiva normativa futura aponta para uma regulação mais sofisticada, baseada em proporcionalidade e segmentação por risco. É provável que o regulador avance na definição normatiza acerca de critérios objetivos para enquadramento de *tokens* como valores mobiliários, na disciplina da custódia digital e na exigência de padrões mínimos de governança e transparência para emissores e plataformas.

No processo de democratização do acesso ao mercado de capitais, a construção de um arcabouço regulatório claro, coerente e estável constitui pressuposto indispensável à consolidação da segurança jurídica. A atuação coordenada da CVM e do Banco Central, aliada à construção progressiva de normas específicas, tende a reduzir assimetrias informacionais e riscos sistêmicos, ao mesmo tempo em que viabiliza modelos inovadores de recursos e investimento.

O desafio regulatório consiste em equilibrar e compatibilizar a proteção ao investidor, estabilidade do sistema financeiro e do mercado de capitais, e o estímulo à inovação. A tokenização, enquanto instrumento tecnológico, não elimina os fundamentos do regime jurídico do mercado de capitais, mas impõe sua reinterpretação à luz de novas estruturas descentralizadas. Assim sendo, o aprimoramento contínuo da regulação e o diálogo institucional entre reguladores e agentes de mercado se relevam determinantes para que a tokenização de ativos cumpra seu potencial de ampliar o acesso a investimentos no Brasil, sem prejuízo da integridade e confiabilidade do sistema.

8. CONSIDERAÇÕES FINAIS

A tokenização de ativos se insere no processo transformação digital dos mercados financeiros, configurando uma evolução substancial nas formas de estruturar, registrar e negociar direitos e valores econômicos. A adoção de tecnologias baseadas em *blockchain* e *smart contracts* não se limita a uma inovação operacional, mas propõe uma reconfiguração das dinâmicas tradicionais de intermediação, liquidação e circulação de ativos, desafiando e reformulando os paradigmas institucionais e regulatórios do mercado de capitais.

Ao conferir o fracionamento de ativos, a redução de custos operacionais e maior eficiência nos processos de liquidação, a tokenização se apresenta como vetor capaz de mitigar barreiras históricas de acesso ao mercado de capitais. A expansão da divisibilidade econômica, aliada à viabilidade de negociação em ambientes digitais contribui para democratização dos investimentos, ampliando a base de investidores e promovendo maior circulação de capital, sem prejuízo da observância à proteção ao investidor e integridade do mercado.

Todavia, a expansão do acesso ao mercado de capitais deve ocorrer de forma condicionada à observância de padrões robustos de transparência, segurança jurídica e mecanismos adequados de proteção ao investidor. A adoção de inovações tecnológicas não exime

os participantes do cumprimento dos deveres de divulgação, da compatibilidade com o perfil de risco dos investidores e da preservação da integridade do mercado. A consolidação de modelos tokenizados depende, portanto, da harmonização entre estímulo à inovação e supervisão regulatória proporcional, assegurando o equilíbrio entre desenvolvimento tecnológico e salvaguardas institucionais.

No contexto brasileiro, a atuação da CVM, como autoridade regulatória principal do mercado de capitais, evidencia que o ordenamento jurídico dispõe de estruturas normativas capazes de absorver as inovações decorrentes da tokenização, desde que observada o teor jurídico inerente das operações.

De forma complementar, o BCB desempenha papel paralelo na supervisão de aspectos relacionados à infraestrutura financeira e à prestação de serviços de ativos virtuais. A evolução normativa tende a consolidar esse enquadramento, conferindo maior previsibilidade e segurança jurídica às iniciativas que utilizam tecnologias de registro distribuído.

Por fim, a tokenização de ativos representa um movimento de modernização compatível com a digitalização da economia e com a busca por maior eficiência no mercado de capitais. Seu desenvolvimento sustentável dependerá da harmonização entre tecnologia, regulação e governança, de modo a assegurar que a ampliação do acesso aos investimentos ocorra de forma segura, transparente e alinhada aos princípios estruturantes do sistema financeiro.

REFERÊNCIAS

AMORIM, K. A. F. de; LUCENA, G. K. F.; GIRÃO, L. F. de A. P.; QUEIROZ, D. B. de. A influência da educação financeira na inserção dos investidores no mercado de capitais brasileiro: um estudo com discentes da área de negócios. **RACE – Revista de Administração, Contabilidade e Economia**, v. 17, n. 2, p. 567–590, 2018. DOI: 10.18593/race.v17i2.16834. Disponível em: <https://periodicos.unoesc.edu.br/race/article/view/16834>. Acesso em: 15 de janeiro de 2026.

ANBIMA. **Tokenização de ativos**. Disponível em: <https://www.anbima.com.br/data/files/02/30/82/CB/68001810C27A8F08882BA2A8/Tokenizacao%20de%20ativos.pdf>. Acesso em: 15 de janeiro de 2026.

ANBIMA – ASSOCIAÇÃO BRASILEIRA DAS ENTIDADES DOS MERCADOS FINANCEIRO E DE CAPITAIS. **Estudo da ANBIMA mostra contribuição do mercado de capitais para o desenvolvimento econômico brasileiro**. Disponível em: <https://www.anbima.com.br/data/files/8E/B4/5C/C7/F26C7910C05C4A79B82BA2A8/A%20contribui%C3%A7%C3%A3o%20do%20mercado%20de%20capitais%20para%20o%20desenvolvimento%20econ%C3%B4mico.pdf>. Acesso em: 15 de janeiro de 2026.

ANBIMA – ASSOCIAÇÃO BRASILEIRA DAS ENTIDADES DOS MERCADOS FINANCEIRO E DE CAPITAIS. **Relatório de Diversidade ANBIMA 2025**. São Paulo: ANBIMA, 2025. Disponível em: https://www.anbima.com.br/data/files/CC/13/FA/04/59DE89100C12BE89B82BA2A8/Relatorio_Diversidade_Anbima_2025.pdf. Acesso em: 15 de janeiro 2026.

ARAUJO. Danilo Borges dos Santos Gomes de. **Regulação Brasileira do Mercado de Capitais**. São Paulo: Saraiva, 2015, p. 31.

ASA – Análise CVM. **Investidores no mercado de capitais brasileiro**. Brasília: CVM, 19 jul. 2021. Disponível em: <https://www.gov.br/cvm/>

pt-br/centrais-de-conteudo/publicacoes/estudos/air_investidores-no-mercado-de-capitais-brasileiro_2021-07-19.pdf. Acesso em: 15 de janeiro de 2026.

B3. Tokenização de ativos: o que é, como funciona e quais seus benefícios. Disponível em: <https://borainvestir.b3.com.br/tipos-de-investimentos/renda-variavel/criptoativos/tokenizacao-de-ativos-o-que-e-como-funciona-e-quais-seus-beneficios/>. Acesso em: 15 de janeiro de 2026.

B3. Volume médio diário de negociação no mercado à vista na B3 atinge R\$ 29 bilhões, alta de 3,4 % em 12 meses, revela DataWise+. São Paulo: B3, 12 dez. 2025. Disponível em: <https://www.b3.com.br/pt-br/noticias/volume-medio-diario-de-negociacao-no-mercado-a-vista-na-b3-atinge-r-29-bilhoes-alta-de-3-4-em-12-meses-revela-datawise.htm>. Acesso em: 15 de janeiro de 2026.

BRASIL. Comissão de Valores Mobiliários (CVM). **Resolução CVM nº 88, de 27 de abril de 2022.** Regulamenta a oferta pública de distribuição de valores mobiliários de emissão de sociedades empresárias de pequeno porte realizada com dispensa de registro por meio de plataforma eletrônica de investimento participativo. Disponível em: <https://conteudo.cvm.gov.br/export/sites/cvm/legislacao/resolucoes/anexos/001/resol088consolid.pdf>. Acesso em: 20 de janeiro de 2026.

BRASIL. **Decreto nº 11.563, de 13 de junho de 2023.** Regulamenta a Lei nº 14.478, de 21 de dezembro de 2022, que dispõe sobre diretrizes para a prestação de serviços relacionados a criptoativos. 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11563.htm. Acesso em: 20 de janeiro de 2026.

BRASIL. **Lei nº 4.595, de 31 de dezembro de 1964.** Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L4595.htm. Acesso em: 15 de janeiro de 2026.

BRASIL. **Lei nº 6.385, de 7 de dezembro de 1976.** Disponível em: https://www.planalto.gov.br/ccivil_03/Leis/L6385.htm. Acesso em: 15 de janeiro de 2026.

BRASIL. **Lei nº 14.430, de 3 de agosto de 2022.** Dispõe sobre o Certificado de Recebíveis do Agronegócio (CRA) e o Certificado de Recebíveis Imobiliários (CRI), institui o Certificado de Recebíveis Gerais e altera as Leis nº 8.668, de 25 de junho de 1993, nº 9.514, de 20 de novembro de 1997, e nº 10.931, de 2 de agosto de 2004. 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2022-2026/2022/lei/L14430.htm. Acesso em: 20 de janeiro de 2026.

BRASIL. **Lei nº 14.478, de 21 de dezembro de 2022.** Dispõe sobre diretrizes para a prestação de serviços relacionados a criptoativos no Brasil. 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2022-2026/2022/lei/L14478.htm. Acesso em: 20 de janeiro de 2026.

CHEN, Yihan. **The sharing economy: analyses and perspectives from an economic perspective. International Journal of Information Management**, v. 43, p. 328–341, 2018. Disponível em: <https://doi.org/10.1016/j.ijinfomgt.2018.07.004>. Acesso em: 15 de janeiro de 2026.

COMISSÃO DE VALORES MOBILIÁRIOS (CVM). **Boletim Econômico – 3º trimestre de 2025: FII, FIDC e crowdfunding são destaques no terceiro trimestre de 2025.** Brasília: CVM, 28 out. 2025. Disponível em: <https://www.gov.br/cvm/pt-br/assuntos/noticias/2025/fii-fidc-e-crowdfunding-sao-destaques-no-terceiro-trimestre-de-2025>. Acesso em: 20 de janeiro de 2026.

COMISSÃO DE VALORES MOBILIÁRIOS (CVM). **Parecer de Orientação CVM nº 40, de 11 de outubro de 2022.** Disponível em: <https://conteudo.cvm.gov.br/legislacao/pareceres-orientacao/pare040.html>. Acesso em: 15 de janeiro de 2026.

COMISSÃO DE VALORES MOBILIÁRIOS – CVM. **Resolução CVM nº 175, de 23 de dezembro de 2022.** Disponível em: <https://conteudo.cvm.gov.br/export/sites/cvm/legislacao/resolucoes/anexos/100/resol175.pdf>. Acesso em: 15 de janeiro de 2026.

GFMA; BOSTON CONSULTING GROUP; ASHURST; SULLIVAN & CROMWELL. **The Impact of DLT in Capital Markets: Ready for Adoption, Time to Act.** Joint Trades Report, 19 Aug. 2025. Disponível em: <https://www.gfma.org/policies-resources/joint-trades-publish-report-on-the-impact-of-dlt-in-capital-markets/> . Acesso em: 15 de janeiro de 2026.

GLOBAL DIGITAL ECONOMY REPORT 2025. **The digital economy comprises about 15 % of world GDP and accounts for approximately USD 16 trillion in 2024.** IDC-A, 2025. Disponível em: <https://www.idc-a.org/insights/qUi9XgvyrzSkyDUy9Tqr>. Acesso em: 15 de janeiro de 2026.

GUERREIRO, José Alexandre Tavares; BUSCHINELLI, Gabriel Saad Kik. **ICOs (Initial Coin Offerings) e a Disciplina dos Valores Mobiliários.** In: Alexandre Evaristo Pinto; Pedro Eroles; Roberto Quiroga Mosquera, em coordenação. *Criptoativos – Estudo Regulatórios e Tributários*. São Paulo: Quartier Latin, 2021. p. 467-486.

HAMARI, Juho; SJÖKLINT, Mimmi; UKKONEN, Antti. **The Sharing Economy: Why People Participate in Collaborative Consumption.** *Journal of the Association for Information Science and Technology*, v. 67, p. 2047-2059, Set 2016, DOI 10.1002/asi.23552, ISSN 2330-1643. Disponível em: <https://www.researchgate.net/publication/255698095>. Acesso em: 15 de janeiro de 2026.

HU, Yining; LIYANAGE, Madhusanka; MANSOOR, Ahsan; THILAKARATHNA, Kanchana; JOURJON, Guillaume; SENEVIRATNE, Aruna. **Blockchain-based Smart Contracts - Applications and**

Challenges. Disponível em: <https://arxiv.org/abs/1810.04699>. Acesso em: 15 de janeiro de 2026.

IOSCO — International Organization of Securities Commissions. Tokenization of Financial Assets. Pub. Doc. 809, 2025. Disponível em: <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD809.pdf>. Acesso em: 20 de janeiro de 2026.

KIKTENKO, EO. et al. **Quantum-secured blockchain.** Quantum Science and Technology, IOP Publishing, v. 3, n. 3, p. 8, 2018.

MAFRUR, Rischian. **Tokenize Everything, But Can You Sell It? RWA Liquidity Challenges and the Road Ahead.** arXiv, 03 ago. 2025. Disponível em: <https://arxiv.org/abs/2508.11651>. Acesso em: 20 de janeiro de 2026.

MATOS, Daniel Oliveira. **Aspectos econômicos dos criptotativos e a valoração de preço com base no fluxo de dados.** In: Daniel de Paiva Gomes; Eduardo de Paiva Gomes; Paulo Cesar Conrado, em coordenação. Criptoativos, Tokenização, Blockchain e Metaverso: aspectos filosóficos, tecnológicos, jurídicos e econômicos. São Paulo: Thomson Reuters Brasil, 2022. p. 363-364.

MCKINSEY & COMPANY. **Tokenized financial assets: From pilot to scale — The transformational power of tokenizing assets.** McKinsey & Company, 2024. Disponível em: <https://www.mckinsey.com.br/en/industries/financial-services/our-insights/from-ripples-to-waves-the-transformational-power-of-tokenizing-assets>. Acesso em: 15 de janeiro de 2026.

NAKAMOTO, Satoshi. **Bitcoin: A Peer-to-Peer Electronic Cash System. 2008.** Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 15 de janeiro de 2026.

OCDE. **The tokenisation of assets and potential implications for financial markets.** OECD Blockchain Policy Series, 2020.

OECD – Organisation for Economic Co-operation and Development. **The Tokenisation of Assets and Potential Implications for Financial Markets.** OECD Blockchain Policy Series, Paris: OECD, 2020. Disponível em: <https://www.blockchainwg.eu/wp-content/uploads/2020/03/The-Tokenisation-of-Assets-and-Potential-Implications-for-Financial-Markets.pdf>. Acesso em: 20 de janeiro de 2026.

PRECEDENCE RESEARCH. **Peer-to-Peer (P2P) lending market size to exceed USD 1,380.80 billion by 2034 driven by digitalization and fintech adoption.** Globe Newswire, 05 set. 2025. Disponível em: <https://www.globenewswire.com/news-release/2025/09/05/3145304/0/en/Peer-to-Peer-P2P-Lending-Market-Size-to-Exceed-USD-1-380-80-Billion-by-2034-Driven-by-Digitalization-and-Fintech-Adoption.html> . Acesso em: 15 de janeiro de 2026.

ROVAI, Armando Luiz; SILVA, André Luis Caetano. **Possibilidade jurídica de integralização do capital social através de criptomoeda e ativos similares.** In: Alexandre Evaristo Pinto; Pedro Eroles; Roberto Quiroga Mosquera, em coordenação. Criptoativos – Estudo Regulatórios e Tributários. São Paulo: Quartier Latin, 2021. p. 531-533.

SUPREMA CORTE DOS ESTADOS UNIDOS. **SEC v. WJ Howey Co.**, 328 US 293, 1946.

VITÓRIA, G. M., Araújo Neto, M. J. de, Pinto, D. S. A., & Pereira, V. P. (2025). **OS IMPACTOS SOCIOECONÔMICOS DAS CRIPTOMOEDAS E DA TECNOLOGIA BLOCKCHAIN NO FUTURO DO BRASIL: DESAFIOS E OPORTUNIDADES.** REVISTA FOCO, 18(11), e10668. Disponível em: <https://doi.org/10.54751/revistafoco.v18n11-187>. Acesso em: 20 de janeiro de 2026.

WORLD ECONOMIC FORUM. **Asset Tokenization in Financial Markets: The Next Generation of Value Exchange.** 21 May 2025. Disponível em: <https://www.weforum.org/publications/>

asset-tokenization-in-financial-markets-the-next-generation-of-value-exchange/. Acesso em: 20 de janeiro de 2026.

WORLD ECONOMIC FORUM. **New study finds financial education gaps are primary barrier to retail investing in capital markets.** 04 ago. 2022. Disponível em: <https://www.weforum.org/press/2022/08/new-study-finds-financial-education-gaps-are-primary-barrier-to-retail-investing-in-capital-markets/>. Acesso em: 15 de janeiro de 2026.

YAZBEK, Otávio. **Regulação do Mercado Financeiro e de Capitais.** Rio de Janeiro: Elsevier. 2007, p. 259.

7. A PENHORA DE CRIPTOATIVOS NO BRASIL

Larissa Celestino Teles

Especialista em Direito Digital pelo Instituto de Tecnologia e Sociedade do Rio de Janeiro – ITS Rio em parceria com o Centro de Estudos e Pesquisas no Ensino do Direito da Universidade do Estado do Rio de Janeiro (CEPED/UERJ). Bacharel em Direito pela Universidade do Estado do Rio de Janeiro (UERJ). Integra a equipe de Ativos Digitais, Blockchain Web3 do Villemor Amaral Advogados. Profissional Certificada CEAV/ABCRIPTO Especialista em Ativos Virtuais.

INTRODUÇÃO

Nos últimos anos, a ascensão dos criptoativos vem transformando de maneira significativa o cenário financeiro global. Segundo pesquisa realizada pela Chainalysis, entre julho de 2022 e junho de 2025, a América Latina registrou quase 1,5 trilhão de dólares em volume de transações com criptomoedas¹⁶³.

Essa realidade tem ganhado contornos cada vez mais expressivos no Brasil, uma vez que esse responde por aproximadamente um terço de todo o volume transacionado na América Latina, sendo o líder LATAM¹⁶⁴ em adoção de criptoativos, o que coloca o país na quinta posição no *ranking* mundial de adoção de criptomoedas¹⁶⁵. Esse

163 “Entre julho de 2022 e junho de 2025, a América Latina registrou quase US\$ 1,5 trilhão em volume de transações com criptomoedas, consolidando a região como uma das mais dinâmicas do mundo.” **CHAINALYSIS**. *Latin America is one of the world’s most dynamic crypto markets*. Disponível em: <https://www.chainalysis.com/blog/latin-america-crypto-adoption-2025/>. Acesso em: 12 out. 2025.

164 Abreviação do termo “Latin America”. **CAMBRIDGE DICTIONARY**. *LatAm*. Disponível em: <https://dictionary.cambridge.org/pt/dicionario/ingles/latam>. Acesso em: 12 out. 2025.

165 “O ecossistema de criptomoedas mais amplo da América Latina. O Brasil domina a região da América Latina, com US\$ 318,8 bilhões em valor recebido em criptomoedas, respondendo por quase um terço de toda a atividade cripto da região.” **CHAINALYSIS**. *Latin America is one of the world’s most dynamic crypto markets*. Disponível em: <https://>

cenário, impõe desafios urgentes ao ordenamento jurídico pátrio, especialmente no que diz respeito à efetividade das decisões judiciais.

Com o aumento do uso de criptoativos, torna-se cada vez mais comum a existência desses bens como parte significativa do patrimônio dos devedores. Apesar dessa realidade, o Brasil ainda não possui dentro do seu ordenamento jurídico mecanismos claros, eficazes e padronizados que permitam a localização, o bloqueio e a penhora judicial desses ativos.

A natureza descentralizada dos criptoativos, a multiplicidade de plataformas que oferecem serviços relacionados, bem como a ausência de regulamentação específica sobre sua apreensão judicial, dificulta a atuação do poder judiciário e podem comprometer o direito dos credores à satisfação de seus créditos.

Dessa forma, torna-se imprescindível que o ordenamento jurídico brasileiro se adeque à nova realidade digital, incorporando mecanismos eficazes para sua penhora nos casos de execução.

Nesse sentido cabe sinalizar que – atualmente – está em fase de criação o sistema Criptojud, que visa permitir a comunicação direta entre o Poder Judiciário e as *exchanges* de criptoativos, viabilizando a identificação, o bloqueio e a transferência desses bens no âmbito judicial. A criação desse sistema, embora represente um avanço necessário, possui diversos desafios a serem enfrentados, dentre esses: a padronização das comunicações com as *exchanges*; a identificação precisa dos titulares dos ativos; a volatilidade dos valores envolvidos e as especificidades técnicas das diversas espécies de criptoativos.

Diante desse cenário, torna-se imprescindível compreender os elementos fundamentais que caracterizam esses ativos, sua natureza jurídica e sua operacionalização no ambiente digital, o que será objeto de análise nos próximos capítulos.

1. CONCEITOS INICIAIS

1.1 Moeda

Antes de abordar o conceito de criptoativo, é necessário compreender outro conceito fundamental para a economia: o de moeda, que - embora presente no cotidiano de todas as sociedades conhecidas - constitui um fenômeno conceitualmente complexo. Por esse motivo, sua definição costuma se basear principalmente em suas propriedades essenciais: reserva de valor, meio de pagamento e propriedade de conta¹⁶⁶.

Alguns autores apresentam essas funções com variações terminológicas. É o caso do pós-doutor em inteligência artificial Cristian Aranha, que, em seu livro, define moeda como: reserva de valor – entendida como meio de transferir o poder de compra para uma futura transação; medida de valor – como uma unidade comum de contagem, ou seja, o padrão de medida estabelecido para quantificar preços e serviços; e meio de troca – como algo utilizado na aquisição de bens ou serviços, de vendedores por compradores¹⁶⁷.

Em síntese, trata-se de visões que partem da mesma base teórica, com diferenças terminológicas. De forma semelhante o autor Gustavo Cunha resume a ideia central de moeda com clareza: “*Em outras palavras, tem que ser aceita para pagarmos itens que desejamos, ser divisível para podermos fazer contas com ela e poder ser guardada sem perder o valor*”¹⁶⁸.

Essas propriedades, contudo, não existem de forma isolada: elas dependem de reconhecimento social e de um grau mínimo de confiabilidade por parte dos indivíduos que utilizam o sistema monetário. Nesse sentido, o autor Sergio Zahr Filho destaca, com precisão:

166 **CUNHA, Gustavo.** *A tokenização do dinheiro*. São Paulo: Almedina Brasil, 2024. p. 46.

167 **ARANHA, Cristian.** *Bitcoin, blockchain e muito dinheiro*. 4. ed. Rio de Janeiro: Valentina, 2022. fls. 31-32

168 **CUNHA, Gustavo.** *A tokenização do dinheiro*. São Paulo: Almedina Brasil, 2024. p. 46.

A moeda é capaz de exercer todas essas funções, **pois os membros de uma dada comunidade a reconhecem como padrão de valor confiável dos bens e serviços produzidos naquele ambiente**, sendo por isso mesmo capaz de suportar **quaisquer transações de conteúdo econômico naquela comunidade. Nesse sentido, a moeda é instituição social que possibilita as relações de trocas da economia de mercado.** (grifo nosso)¹⁶⁹.

A confiabilidade e o reconhecimento social por parte da comunidade são imprescindíveis para que haja a aceitação e o uso da moeda dentro do escopo de suas atribuições. Fala-se, portanto, de fideducía (fé) na moeda, que pode ser decorrente de diferentes escolhas narrativas. O real, por exemplo, é uma moeda emitida de maneira centralizada pelo governo que garante a sua validade e o seu valor de forma que a sociedade aceita essa realidade, sendo assim uma moeda fiduciária.

1.2 Os inúmeros conceitos de moeda

Um erro recorrente é a utilização dos termos moeda eletrônica, moeda virtual, moeda digital e criptomoeda como sinônimos, quando, na verdade, são conceitos distintos.

A moeda eletrônica, por exemplo, refere-se à conversão de uma moeda originalmente emitida em formato físico ou escritural para o meio eletrônico. É, portanto, uma moeda emitida por ente público, regulada no âmbito nacional, centralizada e com curso forçado¹⁷⁰ (esse último referente à moeda, e não ao meio). Esse termo está presente na Lei nº 12.865, de 2013, que, entre outros pontos, dispõe

169 **FILHO, Sergio Zahr.** *Penhora: exame da técnica processual à luz da realidade econômica social*. Faculdade de Direito da Universidade de São Paulo, São Paulo, 2009. Disponível em: https://teses.usp.br/teses/disponiveis/2/2137/tde-15062011-162250/publico/DISSERTACAOFINAL_CD_.pdf. fls. 123. Acesso em: 21 set. 2025.

170 “As moedas de curso forçado dão aquelas que os governos determinam como sendo de aceitação geral em seu território. Esse tipo de moeda não possui valor em si mesma; ela é um tanto simbólica, e sua aceitação depende do grau de confiança por parte da população. **ARANHA, Cristian.** *Bitcoin, blockchain e muito dinheiro*. 4. ed. Rio de Janeiro: Valentina, 2022. fl. 49.

sobre os arranjos de pagamento e sobre as instituições de pagamento integrantes do Sistema de Pagamentos Brasileiro (SPB).

Art. 6º Para os efeitos das normas aplicáveis aos arranjos e às instituições de pagamento que passam a integrar o Sistema de Pagamentos Brasileiro (SPB), nos termos desta Lei, considera-se: (...)

III - instituição de pagamento - pessoa jurídica que, aderindo a um ou mais arranjos de pagamento, tenha como atividade principal ou acessória, alternativa ou cumulativamente: (...)

g) converter moeda física ou escritural em **moeda eletrônica**, ou vice-versa, credenciar a aceitação ou gerir o uso de moeda eletrônica; e

(...)

VI - **moeda eletrônica - recursos armazenados em dispositivo ou sistema eletrônico que permitem ao usuário final efetuar transação de pagamento.** (grifo nosso)¹⁷¹

Nesse caso, é possível identificar com clareza que há uma conversão de uma moeda existente para a moeda eletrônica, sendo responsabilidade da Instituição de Pagamento a gestão dessa, a fim de evitar o problema do duplo gasto - ou seja, a possibilidade de que uma mesma moeda - por exemplo, um real - seja utilizada mais de uma vez, assumindo, no exemplo, a função de dois reais.

Cabe sinalizar o entendimento de Sérgio Zahir Filho:

Para tanto, a moeda se exterioriza nos meios ou instrumentos de pagamentos que podem ser tangíveis, tal como é o papel-moeda, ou intangíveis, tal como é a moeda escritural, representada por lançamentos escriturais em contas bancárias, e a **chamada moeda eletrônica que circula na economia por sistemas bancários**

171 **BRASIL.** *Lei nº 12.865, de 9 de outubro de 2013.* Dispõe sobre o arranjo de pagamento e as instituições de pagamento integrantes do Sistema de Pagamentos Brasileiro. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12865.htm. Acesso em: 15 out. 2025.

informatizados, suportados em senhas, comandos eletrônicos, cartões de débito, etc¹⁷². (grifo nosso)

A moeda virtual, por sua vez, não é desenvolvida por um ente central, sendo normalmente controlada pelos próprios desenvolvedores, como é o caso, por exemplo, de moedas criadas para serem utilizadas dentro de jogos eletrônicos. Nesse sentido, destaca-se o entendimento do Banco Central Europeu (*European Central Bank*), que, em 2012, publicou o relatório intitulado *Virtual Currency Schemes* (em tradução livre, “Esquemas de Moedas Virtuais”), no qual não apenas definiu o conceito de moeda virtual, mas também estabeleceu seus subtipos e diferenciou-a da moeda eletrônica.

Uma moeda virtual pode ser definida como um tipo de dinheiro digital não regulamentado, que é emitido e geralmente controlado por seus desenvolvedores, e usado e aceito entre os membros de uma comunidade virtual específica. Dependendo de sua interação com o dinheiro tradicional, “real”, e com a economia real, os esquemas de moeda virtual podem ser classificados em três tipos: Tipo 1, que é usado para se referir a esquemas de moeda virtual fechados, basicamente usados em um jogo online; esquemas de moeda virtual do Tipo 2 possuem um fluxo unidirecional (geralmente um influxo), ou seja, há uma taxa de conversão para a compra da moeda virtual, que pode subsequentemente ser usada para comprar bens e serviços virtuais, mas, excepcionalmente, também para comprar bens e serviços reais; e os esquemas de moeda virtual do Tipo 3 possuem fluxos bidirecionais, ou seja, a moeda virtual, nesse caso, atua como qualquer outra moeda conversível, com duas taxas de câmbio (compra e venda), podendo subsequentemente ser usada para comprar bens e serviços virtuais, mas também para adquirir bens e serviços reais.

Os esquemas de moeda virtual diferem dos esquemas de dinheiro eletrônico na medida em que a moeda usada como unidade

172 **FILHO, Sérgio Zahr.** *Penhora: exame da técnica processual à luz da realidade econômica social*. Faculdade de Direito da Universidade de São Paulo, São Paulo, 2009. Disponível em: https://teses.usp.br/teses/disponiveis/2/2137/tde-15062011-162250/publico/DISSERTACAOFINAL_CD_.pdf. fl. 124. Acesso em: 21 set. 2025.

de conta não possui um equivalente físico com status de curso legal.
(...) (tradução livre, grifo nosso)¹⁷³.

De todos os conceitos abordados, o mais controvertido é o de moeda digital, que ora aparece como um conceito mais amplo em relação aos demais - ou seja, a ideia de que tanto a moeda eletrônica quanto a moeda virtual estariam abarcadas sob o conceito de moeda digital - ora surge associado ao entendimento de digitalização da moeda física e escritural, sendo, portanto, considerado um sinônimo de moeda eletrônica.

O entendimento que parece ser o mais viável, parte da análise do termo “digital”. Concerne da ideia de que a moeda digital resulta do fim do período analógico e do início da era digital e, portanto, corresponderia à moeda digitalizada *lato sensu*. Aqui, não importa qual seja a natureza da moeda, mas sim o fato dela estar inserida em um ambiente digital. A moeda digital poderia ser, portanto, o conceito guarda-chuva que engloba as demais formas mencionadas, uma vez que todas operam em meio digital.

As criptomoedas, por sua vez, são representações criptografadas de valor que utilizam a chamada DLT (*Distributed Ledger Technology* - tecnologia de registro distribuído), com o objetivo de garantir segurança, rastreabilidade e auditabilidade às operações. Vale destacar

173 “A virtual currency can be defined as a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community. Depending on their interaction with traditional, “real” money and the real economy, virtual currency schemes can be classified into three types: Type 1, which is used to refer to closed virtual currency schemes, basically used in an online game; Type 2 virtual currency schemes have a unidirectional flow (usually an inflow), i.e. there is a conversion rate for purchasing the virtual currency, which can subsequently be used to buy virtual goods and services, but exceptionally also to buy real goods and services; and Type 3 virtual currency schemes have bidirectional flows, i.e. the virtual currency in this respect acts like any other convertible currency, with two exchange rates (buy and sell), which can subsequently be used to buy virtual goods and services, but also to purchase real goods and services. Virtual currency schemes differ from electronic money schemes insofar as the currency being used as the unit of account has no physical counterpart with legal tender status. The absence of a distinct legal framework leads to other important differences as well.”
ECB – EUROPEAN CENTRAL BANK. Virtual currency schemes. October 2012. Disponível em: <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>. Acesso em: 15 out. 2025.

que a DLT é um gênero do qual o *blockchain* é uma espécie, tema que será aprofundado em capítulo específico deste trabalho.

Ainda nesse sentido, cabe destacar que toda criptomoeda é uma moeda digital (por estar em um meio digital), mas nem toda moeda digital é uma criptomoeda, conforme os pontos já expostos¹⁷⁴.

2.2 Criptomoeda

Compreendido o conceito de moeda, pode-se passar à definição de criptomoeda, que corresponde a um sistema de contabilização para criação e circulação de valores, baseado em tecnologias de criptografia ponta a ponta (fim-a-fim) e *blockchain*¹⁷⁵.

Uma dúvida que é frequentemente levantada é se as criptomoedas podem ser efetivamente consideradas moedas, já que, segundo alguns estudiosos, não atendem às três funções essenciais - já mencionadas - da moeda tradicional (reserva de valor, unidade de conta e meio de troca).

Nesse sentido, à exemplo, cabe elaborar a ideia com base no Bitcoin, que embora aceite como meio de pagamento em alguns estabelecimentos e, portanto, considerado um meio de troca, não é utilizado como método de precificação primário, tendo seu valor de mercado geralmente expresso em relação a moedas fiduciárias, como o dólar¹⁷⁶.

174 **CNN BRASIL.** Entenda a diferença entre criptomoeda e moeda digital, como a estudada pelo BC. Disponível em: <https://www.cnnbrasil.com.br/economia/financas/entenda-a-diferenca-entre-criptomoeda-e-moeda-digital-como-a-estudada-pelo-bc/>. Acesso em: 15 out. 2025.

175 “sistema de contabilização de criação e circulação de valores que emprega criptografia fim-a-fim e blockchains para obter características (resistência a adulteração, auditabilidade universal independente, descentralização, contabilização perfeita) que não são possíveis de outra forma.” **ABCRIPTO.** Glossário ABCRIPTO. Versão 1.1, 03 jul. 2023. Disponível em: https://backend.abcripto.com.br/media/files/documentsDownloadSection/glossario_abcripto_v1.pdf. fl. 17. Acesso em: 16.out. 2025.

176 Muitos argumentam que, como quase ninguém precifica nativamente bens e serviços em criptomoedas, elas não cumprem a função de “unidade de conta”. Até existem mercados virtuais onde os preços dos bens e serviços são exibidos em unidades de criptomoedas (bitcoin, por exemplo), mas sempre calculados em função

No entanto, para alguns estudiosos o Bitcoin seria a primeira moeda descentralizada da história¹⁷⁷, devido ao uso do sistema *blockchain*¹⁷⁸, que permite a auditabilidade das informações, não estando focada em um ente centralizado.

Em virtude de sua natureza descentralizada e da ausência de controle por parte de uma autoridade estatal, o Bitcoin pode ser classificado como uma moeda privada. Por esse motivo, sua cotação está sujeita a variações conforme as dinâmicas do mercado¹⁷⁹, o que compromete uma de suas principais funções econômicas: a reserva de valor. Essas variações colocam em xeque a ideia de reserva de valor que é uma das características precípuas da moeda. No entanto, esse entendimento, desconsidera contextos específicos, como os de hiperinflação vivenciados por determinados Estados-nação, nos quais populações locais passam a adotar moedas estrangeiras mais estáveis em suas transações cotidianas. Ainda nesses cenários, a moeda nacional permanece sendo moeda, ainda que perca parte da sua característica de reserva de valor.

Nesses cenários, historicamente, a moeda comumente utilizada como alternativa é o dólar norte-americano. No entanto, em 2021,

de um preço base em moeda nacional (dólar americano, tipicamente), multiplicado pelo preço da criptomoeda nas corretoras naquele instante. Como o preço das criptomoedas é muito volátil, variando significativamente em questão de horas, não há como fazer os preços dos bens e serviços parecerem estáveis. **ABCRIPTO**. *Glossário ABCRIPTO*. Versão 1.1, 03 jul. 2023. Disponível em: https://backend.abcripto.com.br/media/files/documentsDownloadSection/glossario_abcripto_v1.pdf. fl. 17. Acesso em: 21 set. 2025.

177 “De modo geral, podemos afirmar que o Bitcoin surgiu como a primeira criptomoeda descentralizada da história.” **ARANHA, Cristian**. *Bitcoin, blockchain e muito dinheiro*. 4. ed. Rio de Janeiro: Valentina, 2022. fls.77

178 “Uma criptomoeda é um meio de troca, centralizado ou descentralizado, que se utiliza da tecnologia de Blockchain e da criptografia para assegurar a validade das transações e a criação de novas unidades da moeda. O Bitcoin foi a primeira criptomoeda descentralizada criada e hoje é o ativo mais valorizado entre seus pares.” **XP INVESTIMENTOS**. O que é uma criptomoeda? Disponível em: <https://atendimento.xpi.com.br/artigo/2169-o-que-e-uma-criptomoeda>. Acesso em: 15 out. 2025.

179 “Uma moeda privada tem um funcionamento distinto das moedas oficiais. Seu valor oscila de acordo com o mercado. O Bitcoin pode ser considerado uma moeda privada.” **ARANHA, Cristian**. *Bitcoin, blockchain e muito dinheiro*. 4. ed. Rio de Janeiro: Valentina, 2022. fls. fls. 35

um caso atípico ganhou destaque: El Salvador tornou-se o primeiro país a reconhecer o Bitcoin como moeda de curso legal, por meio da promulgação da chamada “Lei Bitcoin”. Essa medida representou um marco inédito no cenário global. Entretanto, quatro anos após sua implementação, a referida legislação foi revogada em decorrência de um acordo de empréstimo firmado com o Fundo Monetário Internacional (FMI), o qual estabeleceu como condição a retirada do Bitcoin do ordenamento jurídico monetário do país¹⁸⁰.

É fato que o Bitcoin já vem sendo utilizado como reserva de valor em alguns países, especialmente naqueles cuja moeda local apresenta significativa fragilidade. Nesse cenário, é possível sustentar que o Bitcoin pode ser considerado uma moeda, uma vez que pode ser aceito na aquisição de bens e serviços (meio de pagamento), possui divisibilidade (propriedade de conta) e, apesar de sua volatilidade, pode ser utilizado como reserva de valor.

2.3 Criptoativos ou ativos virtuais

De modo semelhante, o conceito de criptoativo também é objeto de diversas discussões, sendo frequentemente tratado como sinônimo de criptomoeada. A Associação Brasileira de Criptoeconomia (ABCripto), por exemplo, define os criptoativos com base na utilização das criptomoeadas como ativos financeiros, entendendo que estas passam a ser classificadas como criptoativos quando empregadas de maneira análoga à de um ativo financeiro.

criptoativos - o uso de criptomoeadas de forma **análoga** a ativos financeiros, cuja posse ou negociação pode ser usada para trazer

180 O Escritório do Bitcoin de El Salvador está celebrando o “Dia do Bitcoin”, o aniversário da entrada em vigor da lei do Bitcoin como moeda de curso legal em setembro de 2021. (...) Experimento com Bitcoin em El Salvador, quatro anos depois, gera resultados mistos. A legislatura de El Salvador revogou a lei do Bitcoin como moeda legal e concordou em não comprar mais Bitcoin com fundos públicos como parte de um acordo de empréstimo de US\$ 1,4 bilhão com o FMI em janeiro. **COINTELEGRAPH**. El Salvador comemora aniversário do Bitcoin em meio a resultados mistos após 4 anos. Disponível em: <https://br.cointelegraph.com/news/el-salvador-bitcoin-anniversary-mixed-results-4-years>. Acesso em: 16 out. 2025.

retornos financeiros ou outros benefícios ao seu detentor¹⁸¹. (grifo nosso)

Em 2024, o Banco Central do Brasil (BACEN) elaborou algumas consultas públicas que visam, em certa medida, criar uma regulamentação para o uso dos criptoativos no Brasil. A CP 109/2024 do Bacen, por exemplo, busca traçar parâmetros regulatórios para as Prestadoras de Serviços de Ativos Virtuais (PSAVs) e os serviços a essas relacionados.

Embora a análise aprofundada dessas consultas públicas seja realizada em capítulo específico, cabe, desde já, destacar a definição de ativos virtuais contida na minuta de resolução da CP nº 109/2024. Nesse sentido, o artigo 2º, inciso II, dispõe o seguinte:

Artigo 2º: Para efeitos desta Resolução, considera-se:

II - **ativo virtual**: a representação digital de valor que pode ser negociada ou transferida por meios eletrônicos, a exemplo de sistema baseado na tecnologia dos registros distribuídos (Distributed Ledger Technology - DLT) ou similar e que pode ser utilizada para a realização de **pagamentos** ou com **propósito de investimento**, conforme o art. 3º da Lei nº 14.478, de 21 de dezembro de 2022 (grifo nosso).

A resolução em comento não apresenta o conceito de criptoativo, mas sim o de ativo virtual, da mesma forma que é tratado no art. 3º da Lei nº 14.478.

Art. 3º Para os efeitos desta Lei, considera-se ativo virtual a **representação digital de valor** que pode ser negociada ou transferida por meios eletrônicos e utilizada para **realização de pagamentos** ou com **propósito de investimento**, não incluídos:

I - moeda nacional e moedas estrangeiras;

181 **ABCRIPTO**. *Glossário ABCRIPTO*. Versão 1.1, 03 jul. 2023. Disponível em: https://backend.abcripto.com.br/media/files/documentsDownloadSection/glossario_abcripto_v1.pdf. fl. 18. Acesso em: 16.out. 2025.

II - moeda eletrônica, nos termos da Lei nº 12.865, de 9 de outubro de 2013;¹⁸²

III - instrumentos que provejam ao seu titular acesso a produtos ou serviços especificados ou a benefício proveniente desses produtos ou serviços, a exemplo de pontos e recompensas de programas de fidelidade; e

IV - representações de ativos cuja emissão, escrituração, negociação ou liquidação esteja prevista em lei ou regulamento, a exemplo de valores mobiliários e de ativos financeiros.

Parágrafo único. Competirá a órgão ou entidade da Administração Pública federal definido em ato do Poder Executivo estabelecer quais serão os ativos financeiros regulados, para fins desta Lei. (grifo nosso)

Nesse contexto, o ativo virtual pode desempenhar duas funções principais: ser utilizado como meio de pagamento ou como instrumento de investimento.

É importante ressaltar que a proposta apresentada pela minuta da consulta pública suscitou reações por parte de algumas *exchanges*, especialmente no que diz respeito à forma taxativa com que o normativo estabelece que os ativos virtuais devem ser enquadrados exclusivamente para esses dois propósitos. Tal delimitação tem gerado controvérsias, uma vez que, na prática, um mesmo ativo pode apresentar múltiplas funcionalidades, sendo possível, por exemplo, que ele seja classificado como um *token* de utilidade. Nessa hipótese, o ativo não se enquadraria no conceito de ativo virtual conforme

182 Essa moeda eletrônica é a moeda física ou escritural no meio eletrônico. Seria o entendimento de digitalização da moeda ou moeda digital. “Art. 6º Para os efeitos das normas aplicáveis aos arranjos e às instituições de pagamento que passam a integrar o Sistema de Pagamentos Brasileiro (SPB), nos termos desta Lei, considera-se: (...) g) converter moeda física ou escritural em moeda eletrônica, ou vice-versa, credenciar a aceitação ou gerir o uso de moeda eletrônica; e (...)” **BRASIL**. Lei nº 12.865, de 9 de outubro de 2013. Dispõe sobre arranjos e instituições de pagamento e institui o Sistema de Pagamentos Brasileiro (SPB). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/112865.htm. Acesso em: 12 out. 2025.

delineado pela minuta, o que poderia gerar insegurança jurídica quanto à sua regulamentação.

Destaca-se um dos exemplos práticos apresentados pela Binance em sua resposta à mencionada consulta pública:

“Um exemplo prático é o do Ether (ETH) na rede Ethereum. Caso um usuário adquira ETH com finalidade de especular sobre seu valor futuro, buscando lucro em sua eventual valorização, há um componente claro de investimento. Em contrapartida, um desenvolvedor que utiliza ETH para pagar taxas da rede (“gas fees”) na implementação de DApps (aplicativos descentralizados) na rede Ethereum está fazendo uso efetivo do Ether como token de utilidade, pois, nesse caso, o criptoativo é utilizado para viabilizar a execução de códigos e a interação com contratos inteligentes. (...)”

A distinção entre ETH como token de utilidade (empregado em taxas de rede e funcionalidades de DApps) e ETH como objeto de especulação (mantido em carteiras para fins de valorização) exemplifica que um mesmo ativo pode se encaixar em diferentes cenários de uso, exigindo análise contextual e dinâmica por parte dos reguladores, de modo que determinar **taxativamente** que Ativo Virtual é aquele usado apenas para investimento ou pagamento, desde logo, pode parecer um equívoco.

Não há, aqui, uma proposta de alteração de texto. Ao invés disso, estes comentários buscam **fomentar a necessidade de fornecimento de parâmetros** para que as PSAVs possam avaliar a qualificação dos ativos ofertados como ativos virtuais. Logo, o BCB, ao conciliar esses diversos parâmetros — **função de uso, frequência de adoção comercial, índices de especulação, liquidez, perfil de volatilidade, entre outros** — poderá fornecer critérios sólidos para auxiliar as PSAVs a avaliarem se o criptoativo será qualificado como ativo virtual para fins da Lei 14.478/2022, isto é, **se é um ativo utilizado para realização de pagamentos ou com propósito de investimento.**¹⁸³ (grifo nosso)

183 **BINANCE HOLDING UY S.A.** Resposta à consulta pública do Banco Central do Brasil. Disponível em: <https://www3.bcb.gov.br/audpub/DetalharAudienciaPage?6&audienciaId=702>. Fls. 24. Acesso em: 12 out. 2025.

A lógica sinalizada pela corretora é que a definição taxativa, sem parâmetros voltados para a natureza do uso do ativo em si, poderá ensejar em dificuldades práticas de enquadramento no texto legal. Assim é proposto parâmetros para o enquadramento no conceito, ao invés de uma compreensão mais taxativa.

A Receita Federal, por sua vez, optou por conceituar o termo criptoativo - ao invés de ativo virtual - através da Instrução Normativa 1.888/2019¹⁸⁴.

Art. 5º Para fins do disposto nesta Instrução Normativa, considera-se:

I - criptoativo: a **representação digital de valor** denominada em sua própria unidade de conta, cujo preço pode ser expresso em moeda soberana local ou estrangeira, transacionado eletronicamente com a utilização de criptografia e de tecnologias de registros distribuídos, **que pode ser utilizado como forma de investimento, instrumento de transferência de valores ou acesso a serviços, e que não constitui moeda de curso legal; e (grifo nosso)**

O conceito da receita, amplia o escopo de ampliação abordando que criptoativo pode ser usado como investimento, instrumento de transferência de valores ou acesso à serviços, esse último seria o seu uso como token de utilidades. Além disso, não pode ser considerada moeda de curso legal, o que mantém de fora as moedas digitalizadas, como o pix, eventuais CDBCs.

Ainda sobre esse tema, a CVM – em 2022 – publicou o parecer de orientação 40 que traz o seguinte entendimento:

Objeto deste Parecer de Orientação

Criptoativos são ativos representados digitalmente, protegidos por **criptografia**, que podem ser objeto de transações executadas e armazenadas por meio de tecnologias de registro distribuído

184 **BRASIL.** Instrução Normativa RFB nº 1.888, de 2019. Disponível em: <https://normasinternet2.receita.fazenda.gov.br/#/consulta/externa/100592/visao/multivigente>. Acesso em: 14 out. 2025.

(Distributed Ledger Technologies – DLTs). **Usualmente, os criptoativos (ou a sua propriedade) são representados por *tokens*, que são títulos digitais intangíveis.** (grifo nosso)¹⁸⁵

Conforme destacado no Parecer de Orientação nº 40 da Comissão de Valores Mobiliários (CVM), os criptoativos, ou os direitos a esses associados, são geralmente representados por *tokens*, que constituem títulos intangíveis. Dessa forma, evidencia-se a necessidade de aprofundar a compreensão acerca da natureza dos *tokens*, identificar quais deles podem ser classificados como criptoativos e, sobretudo, avaliar a possibilidade de sua penhora judicial.

2.4 Tokens

Token é – resumidamente - a representação de um bem ou direito. Traz a Abcripto em seu glossário:

token ❶ (sem equivalente em Português) a **representação de algum bem, valor ou direito**, comumente criada como contrato inteligente ou submoeda dentro de uma outra criptomoeda maior, ou, às vezes, como uma criptomoeda independente; ❷ a representação abstrata de um valor, bem, ou direito.¹⁸⁶ (grifo nosso)

De uma maneira mais simplificada trata-se da representação de algo, que pode ser dividido em dois entendimentos segundo a associação: o primeiro associa essa existência a um contrato inteligente ou a uma moeda dentro de uma moeda maior ou independente; o segundo a uma representação abstrata de um bem, valor ou direito. O conceito de tokenização da entidade segue um sentido semelhante:

tokenização ❶ o processo de criar, em uma rede de criptomoedas, **uma representação de algum ativo ou direito do mundo real**, permitindo sua divisão, transferência, compra, venda ou gestão

185 **COMISSÃO DE VALORES MOBILIÁRIOS (CVM)**. Parecer de Orientação CVM nº 40, de 11 de outubro de 2022. Disponível em: <https://conteudo.cvm.gov.br/legislacao/pareceres-orientacao/pare040.html>. Acesso em: 15 out. 2025.

186 **ABCRIPTO**. Glossário ABCRIPTO. Versão 1.1, 03 jul. 2023. p. 41. Disponível em: https://backend.abcripto.com.br/media/files/documentsDownloadSection/glossario_abcripto_v1.pdf. Acesso em: 16 out. 2025.

usando as características inerentes à criptomoeda (auditabilidade, descentralização, etc.) (grifo nosso)

O entendimento da entidade sobre o tema merece ressalvas, especialmente devido às diferentes naturezas dos *tokens*, que não necessariamente precisam estar associados a uma rede de criptomoedas. Considerando esse aspecto, o conceito apresentado por Gustavo Cunha é mais apropriado, pois explica que a tokenização consiste na conversão de direitos sobre ativos de modo que estes sejam registrados ou armazenados em um sistema *blockchain*¹⁸⁷.

Apesar de ser um entendimento mais adequado, há quem argumente que a visão de Gustavo Cunha ainda não estaria completamente correta, uma vez que é possível que *tokens* sejam registrados em uma DLT (*Distributed Ledger Technology*), sem que esta seja necessariamente uma *blockchain*, que é um tipo específico de DLT (cadeia de blocos).

Cabe destacar o entendimento da Comissão de Valores Mobiliários (CVM) no Parecer de Orientação nº 40, que aponta que “os criptoativos costumam ser designados como *tokens*”¹⁸⁸ e, a partir disso, estabelece critérios funcionais para identificar quais *tokens* podem ser considerados valores mobiliários e, portanto, estariam sob o escopo regulatório da autarquia.

Nesse sentido, o regulador subdivide os *tokens* em três principais tipos: *token* de pagamento (*cryptocurrency* ou *payment token*); *token* de utilidade (*utility token*); e *token* referenciado a ativo (*asset-backed token*). O parecer apresenta essa classificação de forma explicativa:

Inicialmente, a taxonomia seguirá as seguintes categorias:

187 “A tokenização é o processo de converter direitos de um ativo em um token digital que pode ser movido, registrado ou armazenado em um sistema *blockchain*.” **CUNHA**, Gustavo. A tokenização do dinheiro. São Paulo: Almedina Brasil, 2024, fl. 38.

188 “Os criptoativos costumam ser designados como *tokens* e podem desempenhar diversas funções, razão pela qual acadêmicos e reguladores têm buscado formular uma taxonomia, ainda sem um entendimento uniforme sobre a classificação” **CVM**. Parecer de Orientação nº 40, de 11 de outubro de 2022. p. 4. Disponível em: <https://conteudo.cvm.gov.br/legislacao/pareceres-orientacao/pare040.html>. Acesso em: 16 out. 2025.

Token de Pagamento (cryptocurrency ou payment token): **busca replicar as funções de moeda, notadamente de unidade de conta, meio de troca e reserva de valor;**

Token de Utilidade (utility token): utilizado para adquirir ou **acessar** determinados produtos ou serviços;

Token referenciado a Ativo (asset-backed token): **representa** um ou mais ativos, tangíveis ou intangíveis. São exemplos os “security tokens”, as stablecoins, os non-fungible tokens (NFTs) e os demais ativos objeto de operações de “tokenização”.

As categorias citadas acima não são exclusivas ou estanques, de modo que um único criptoativo pode se enquadrar em uma ou mais categorias, a depender das funções que desempenha e dos direitos a ele associados¹⁸⁹. (grifo nosso)

Essa visão da CVM vai de acordo com o entendimento comum do mercado internacional. Em 2021, a OECD (*Organisation for Economic Co-operation and Development* - Organização para a Cooperação e Desenvolvimento Econômico) publicou uma nota técnica, cujo foco era compreender de maneira geral como estava se dando a regulação sobre tokenização de ativos no mercado financeiro mundial, fazendo – assim - um aparato do entendimento internacional de diferentes órgãos reguladores¹⁹⁰. Um que merece destaque é o entendimento da FCA (*Financial Conduct Authority* – Autoridade de Conduta Financeira), que é o Órgão regulador do setor de serviços Financeiros do Reino Unido e que também fez um Guia sobre criptoativos. Nesse guia há a seguinte menção:

Security tokens: esta categoria não muda de maneira significativa em relação à orientação que foi submetida à consulta e refere-se aos tokens que conferem direitos e obrigações semelhantes

189 **CVM.** Parecer de Orientação nº 40, de 11 de outubro de 2022. fls. 4-5. fl.4 e 5. Disponível em: <https://conteudo.cvm.gov.br/legislacao/pareceres-orientacao/pare040.html> Acesso em 16.out.2025

190 **OECD.** Understanding the tokenisation of assets in financial markets. Paris: OECD, 2021. Disponível em: https://www.oecd.org/content/dam/oecd/en/publications/reports/2021/11/understanding-the-tokenisation-of-assets-in-financial-markets_2e657111/c033401a-en.pdf Acesso em 22. Nov.2025

aos investimentos especificados previstos na RAO, excetuando a moeda eletrônica. A moeda eletrônica foi agora removida especificamente da definição de security token, para criar uma categoria separada. Esses tokens permanecem dentro do perímetro regulatório.

E-money tokens: esta categoria refere-se a qualquer **token que se enquadre na definição de moeda eletrônica**. Esses tokens estão sujeitos às EMRs e as empresas devem garantir que possuem as permissões corretas e seguem as regras e regulamentos relevantes. Essa categoria anteriormente estava inserida na categoria de utility tokens. Esses tokens estão sob regulação.

Unregulated tokens: esta categoria refere-se a **qualquer token que não se enquadre na definição de moeda eletrônica nem conceda direitos equivalentes aos investimentos especificados pela RAO**. Isso inclui tokens conhecidos como **utility tokens e exchange tokens**.

Esses tokens podem, por exemplo, ser emitidos de forma centralizada ou descentralizada, conceder acesso a um **bem ou serviço atual ou futuro em uma ou mais redes e ecossistemas, ou serem usados como meio de troca**. Podem ser totalmente transferíveis ou ter transferibilidade restrita. Esses tokens estão fora do perímetro regulatório. (tradução livre: grifo nosso)¹⁹¹

191 “Security tokens: this category does not change materially from the Guidance that we consulted on and refers to those tokens that provide rights and obligations akin to specified investments as set out in the RAO, excluding e-money. We have now specifically removed e-money from the definition of a security token, to create a separate category. These remain within the regulatory perimeter. • E-money tokens: this category refers to any token that reaches the definition of e-money. These tokens are subject to the EMRs and firms must ensure they have the correct permissions and follow the relevant rules and regulations. This category formerly sat within the utility tokens category. These tokens fall within regulation. • Unregulated tokens: this category refers to any token that does not meet the definition of e-money, or provide the same rights as other specified investments under the RAO. This includes tokens referred to as utility tokens, and exchange tokens. • These tokens can, for example, be issued centrally or be decentralised, give access to a current or prospective good or service in one or multiple networks and ecosystems, or be used as a means of exchange. They can be fully transferable or have restricted transferability. These tokens fall outside the regulatory perimeter. **Financial Conduct Authority. Guidance on Cryptoassets: Policy Statement PS19/22.** London: FCA, July 2019.” Disponível em: <https://www.fca.org.uk/publication/policy/ps19-22.pdf> Acesso em 22.nov.2025

O Parecer da CVM também faz outras menções, especialmente sobre uma prática comum no mercado, em grande parte motivada pela Resolução CVM nº 88, que possibilita a oferta pública de pequenas empresas por meio de plataformas de *crowdfunding* de investimentos – segundo a qual o *token* não representa apenas o ativo, mas também um direito de remuneração, assemelhando-se, assim, a uma estrutura de securitização, conferindo inclusive direito a voto¹⁹². Nesses casos, o *token* será considerado um valor mobiliário, estando, portanto, abrangido pela regulação da CVM.

3. BLOCKCHAIN E DLT: CONCEITOS E DIFERENÇAS

Uma das confusões mais significativas no que tange a efetividade de certas definições no mundo cripto se dá em relação ao conceito de *blockchain* e DLT, especialmente em razão da utilização incorreta desse primeiro termo, que muitas vezes é usado como sinônimo do segundo, quando na verdade se trata de uma espécie do qual o sistema DLT é o gênero. A tecnologia *blockchain* é uma das formas mais conhecidas de DLT, ou tecnologia de registro distribuído e, por isso, a constante confusão.

Em termos gerais, a DLT consiste em um sistema digital descentralizado que permite o registro, a validação e a atualização de dados em múltiplos nós (computadores ou servidores) de uma rede, sem a necessidade de uma autoridade central. Conceitua a Abcripto:

DLT ❶ abreviatura de “Distributed Ledger Technology”, veja: ❷ tecnologia de livro-razão distribuído; tecnologia de

192 “Nesse sentido, vale mencionar que a prática de mercado vem demonstrando que um token pode representar não só ativos, como também direitos de remuneração por empreendimento, direito a receber relacionado a estruturas assemelhadas às de securitização, ou, ainda, direito de voto. A esse respeito, notamos que alguns desses modelos aproximam os *tokens* emitidos do conceito de valor mobiliário e, tendo isso em vista, reforçamos que referida taxonomia não se propõe a consolidar uma definição taxativa de cada classificação, tampouco a limitar o alcance desta Autarquia, cuja atuação dependerá da análise dos casos em concreto” **CVM**. Parecer de Orientação nº 40, de 11 de outubro de 2022. fls. 4-5. fl.4 e 5. fl.5. Disponível em: <https://conteudo.cvm.gov.br/legislacao/pareceres-orientacao/pare040.html> Acesso em 16.out.2025

livro-razão distribuído ❶ (“distributed ledger technology” em inglês, frequentemente abreviado “DLT”) termo cunhado após a criação do Bitcoin e seu respectivo blockchain, **para designar uma ampla gama de abordagens ou plataformas de registro/notarização de transações que podem adotar uma ou algumas das características normalmente associados aos blockchains**, como descentralização, contabilização perfeita, auditabilidade externa independente, código aberto, equipotência dos participantes. (grifo nosso)¹⁹³

Já a *blockchain* é uma tecnologia específica que envolve o agrupamento de blocos. Assim, de acordo com a Abcripto, *blockchain* pode ser definida como:

blockchain ❶ um histórico sequencial de transações ou registros de dados/eventos agrupados em blocos (análogo a “edições” de uma revista ou “diário oficial”) que empregam criptografia para criar uma cadeia de verificação de integridade desde a primeira edição até a mais recente, atuando como registro oficial e autoridade final sobre se uma determinada transação ou evento de fato ocorreu ou não. ❷ O histórico de transações de uma criptomoeda específica (p. ex., “o blockchain do Bitcoin”). ❸ A abordagem geral de usar sistemas computacionais baseados em blockchains para registrar fatos, eventos ou transações¹⁹⁴.

A professora Dayana Uhdre muito bem pontua a diferença entre esses dois sistemas:

Essa estrutura descentralizada (de rede e de registro) é o que chamamos de Distributed Ledger Technology (DLT). **A tecnologia blockchain é uma DLT, porém, o que a caracteriza é a compilação dos dados em blocos de informações encadeados**. Eis a razão da nomenclatura blockchain, que em tradução livre significa “cadeias de blocos”. A ligação entre os blocos de informações é feita por meio dos chamados hash, que seriam as “impressões digitais” de cada um dos

193 ABCRIPTO. **Glossário ABCRIPTO**. Versão 1.1, 03 jul. 2023. fl.40 Disponível em: https://backend.abcripto.com.br/media/files/documentsDownloadSection/glossario_abcripto_v1.pdf Acesso em 16.out.2025

194 ABCRIPTO. **Glossário ABCRIPTO**. Versão 1.1, 03 jul. 2023. fl.7 Disponível em: https://backend.abcripto.com.br/media/files/documentsDownloadSection/glossario_abcripto_v1.pdf Acesso em 16.out.2025

blocos. Cada bloco é iniciado com a cópia do hash do bloco anterior, o qual faz a conexão entre ele e o bloco anterior, e ao final terá um hash unívoco seu, que simultaneamente iniciará o bloco seguinte: (...) (grifo nosso)¹⁹⁵.

A *blockchain*, portanto, é uma implementação específica da DLT que organiza os dados em blocos encadeados de forma cronológica e imutável. Cada bloco contém um conjunto de transações e está vinculado ao bloco anterior por meio de uma função criptográfica chamada hash, formando uma cadeia (*chain*) de blocos (*blocks*), o que assegura a integridade e a rastreabilidade das informações

A principal diferença entre a *blockchain* e outras formas de DLT reside na estrutura dos dados e no modelo de consenso adotado. Enquanto a *blockchain* armazena informações em blocos sequenciais e interdependentes, outras DLTs podem utilizar estruturas alternativas, como os grafos acíclicos direcionados (DAGs)¹⁹⁶, nos quais as transações não dependem da confirmação sequencial por blocos, oferecendo maior flexibilidade e, em alguns casos, escalabilidade superior.

Além disso, nem todas as DLTs seguem o modelo de consenso aberto e público, característico das *blockchains* públicas como Bitcoin ou Ethereum. Existem DLTs permissionadas, nas quais os participantes e validadores são previamente autorizados, o que permite maior controle, privacidade e eficiência, sendo especialmente aplicáveis a contextos corporativos ou regulatórios. Em síntese, toda *blockchain* é uma DLT, mas nem toda DLT é uma *blockchain*.

195 CARVALHO, Uhdre, Dayana de. *Blockchain, tokens e criptomoedas: análise jurídica*. São Paulo: Almedina Brasil, 2021. E-book. p.35. ISBN 9786556271859. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9786556271859/>. Acesso em: 16 out. 2025.

196 “Distributed ledger technology is an innovative approach to database management that has transformed how digital transactions are managed. Blockchain operates on a decentralized network, where nodes validate transactions through consensus mechanisms such as proof-of-work, ensuring security and immutability. While blockchain is the most prominent form of DLT, there are alternatives like Directed Acyclic Graph (DAG) that are just as efficient.” **CRUSTLAB**. Comparison of DAG vs Blockchain: Differences, Pros, and Cons. 23rd July 2025. Disponível em: <https://crustlab.com/blog/dag-vs-blockchain/> Acesso em 16.out.2025

4. CUSTÓDIA

A custódia de criptoativos consiste na prática de guarda, proteção e gerenciamento de ativos digitais, sendo um dos elementos centrais da infraestrutura do mercado cripto. Seu objetivo principal é assegurar a integridade e a disponibilidade das chaves privadas, que são os instrumentos criptográficos indispensáveis para movimentar tais ativos.

A custódia pode ser realizada por intermediários especializados¹⁹⁷ ou pelo próprio titular dos ativos (auto-custódia), e a escolha do modelo de custódia impacta diretamente os níveis de segurança, autonomia e responsabilidade assumidos pelo investidor.

4.1 Auto-custódia

A auto-custódia representa a situação em que o próprio titular detém controle total e exclusivo sobre suas chaves privadas, sem intermediação de terceiros. De acordo com a definição da Abcripto, trata-se do cenário em que o proprietário legal ou moral dos ativos mantém integral controle sobre os meios que permitem a transferência de suas criptomoedas¹⁹⁸.

Cabe sinalizar que apesar dessa definição da Abcripto está de acordo com o entendimento geral, o termo “criptomoedas” talvez não seja o ideal, por ser mais restritiva. Uma outra forma de sinalizar isso seria usando o termo *tokens*. Como pontua Gustavo Cunha:

“(...) é hora de abordar um aspecto igualmente crucial neste universo: **a custódia**. Assim como não basta apenas possuir

197 “custodian wallet provider” means an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies.’ 5 **AMID**. - d) item 19. Disponível em: <https://eur-lex.europa.eu/eli/dir/2018/843/oj/eng> Acesso em 16.out.2025

198 “auto-custódia ● situação em que o proprietário legal ou moral detém controle total e exclusivo das chaves privadas que permitem a transferência de suas criptomoedas para outros endereços.” **Glossário ABCRIPTO**. Versão 1.1, 03 jul. 2023. fl.5 Disponível em: https://backend.abcripto.com.br/media/files/documentsDownloadSection/glossario_abcripto_v1.pdf Acesso em 16.ou.2025

um “tesouro”, mas também é essencial saber onde e como guardá-lo com segurança, no mundo da tokenização, ter a posse de um token é a penas metade da equação.”¹⁹⁹ (grifo nosso)

Essa modalidade maximiza a autonomia e a privacidade do usuário, mas exige profundo conhecimento em segurança cibernética, uma vez que a responsabilidade pela guarda segura das chaves recai inteiramente sobre o investidor, incluindo a prevenção contra perda, roubo ou acesso não autorizado.

4.2 Custódia em *exchange*

Por outro lado, muitos usuários optam por custodiar seus ativos em *exchanges* (corretoras), que são empresas especializadas na intermediação de negociações envolvendo criptoativos, oferecendo serviços como compra e venda, custódia e suporte técnico.

Conforme o glossário da Abcripto, as corretoras operam majoritariamente por meio de plataformas digitais (como aplicativos ou sites), agregando segurança operacional às transações, mas também centralizando o controle sobre os ativos, o que implica em confiar a terceiros a guarda das chaves privadas²⁰⁰.

Há também chamadas corretoras descentralizadas, ou *decentralized exchanges* (DEXs), que operam sem uma autoridade central e permitem que as negociações ocorram diretamente entre os usuários, por meio de contratos inteligentes executados em *blockchain*. Nessas plataformas, não há custódia por parte da corretora, pois os ativos permanecem sob o controle dos próprios usuários até o momento da

199 CUNHA, Gustavo. A tokenização do dinheiro. São Paulo: Almedina Brasil, 2024, p. 40.

200 “corretora ❶ empresa especializada na intermediação de negociações (compra e venda) de criptomoedas, agregando segurança operacional e jurídica nas transações, custódia e possivelmente vários outros serviços, oferecidos tipicamente através de um aplicativo e/ ou site na internet acessível pelo navegador.” **Glossário ABCRIPTO**. Versão 1.1, 03 jul. 2023. fl.15 Disponível em: https://backend.abcripto.com.br/media/files/documentsDownloadSection/glossario_abcripto_v1.pdf Acesso em 16.ou.2025

transação, preservando, assim, o princípio da descentralização e da soberania individual sobre os criptoativos²⁰¹.

5. COLD WALLET (ARMAZENAMENTO FRIO) X HOT WALLET (ARMAZENAMENTO QUENTE)

Quanto à forma técnica de armazenamento, destaca-se a distinção entre o armazenamento ou carteira quente (*hot wallet*) e o armazenamento ou carteira fria (*cold wallet*). O armazenamento quente consiste na guarda de chaves privadas em dispositivos conectados à internet, o que permite a realização imediata de transações, mas aumenta a exposição a riscos cibernéticos²⁰².

Já o armazenamento frio refere-se ao uso de dispositivos desconectados ou de difícil acesso remoto, como carteiras físicas (*hardware wallets*) ou meios offline, com foco na segurança, sendo utilizado geralmente para proteger grandes volumes de ativos²⁰³.

A prática mais comum no mercado é a adoção de um modelo híbrido, em que uma pequena parcela dos ativos permanece em *hot wallets* para atender às demandas operacionais diárias, enquanto a

201 “corretora descentralizada ❶ (tipicamente abreviado como “dex”, contração de “decentralized exchange”) plataforma de negociação de criptoativos em que as negociações ocorrem diretamente entre os usuários através de contratos inteligentes em uma blockchain, dispensando uma autoridade central. **Glossário ABCRIPTO**. Versão 1.1, 03 jul. 2023. fl.15 Disponível em: https://backend.abcripto.com.br/media/files/documentsDownloadSection/glossario_abcripto_v1.pdf Acesso em 16.ou.2025

202 “armazenamento quente ❶ ato de armazenar chaves privadas ou informações altamente sensíveis em um computador conectado constantemente à internet, para que as assinaturas digitais e/ou transações de criptomoeda possam ser feitas instantaneamente quando requisitadas.” **Glossário ABCRIPTO**. Versão 1.1, 03 jul. 2023. fl.3 Disponível em: https://backend.abcripto.com.br/media/files/documentsDownloadSection/glossario_abcripto_v1.pdf Acesso em 16.ou.2025

203 “armazenamento frio ❶ ato de armazenar chaves privadas ou informações altamente sigilosas em dispositivos que permanecem a maior parte do tempo desligados, ou cujo acesso e uso requer uma intervenção física (possivelmente demorada) do seu guardião, ou que nem sequer sejam eletrônicos. ❷ o local ou meio físico onde esse armazenamento é feito. ❸ sinônimo informal, mas tecnicamente incorreto, para: ▀ carteira em hardware”. **Glossário ABCRIPTO**. Versão 1.1, 03 jul. 2023. fl.3 Disponível em: https://backend.abcripto.com.br/media/files/documentsDownloadSection/glossario_abcripto_v1.pdf Acesso em 16.ou.2025

maior parte é mantida em cold wallets, com vistas à mitigação de riscos. Esse modelo é amplamente adotado por corretoras e custodiante profissionais, conforme suas políticas internas de gestão de risco²⁰⁴.

6. ASPECTOS REGULATÓRIOS NO BRASIL

O Brasil tem experimentado um amplo processo de desenvolvimento regulatório no ecossistema dos criptoativos. Essa evolução normativa envolve diferentes órgãos reguladores, como a Receita Federal do Brasil, a Comissão de Valores Mobiliários, o Banco Central, além do próprio Congresso Nacional, que contribuem de diferentes formas na construção gradual de um arcabouço legal e infralegal sobre o tema.

7. RECEITA FEDERAL

Em 2019, a Receita Federal publicou a Instrução Normativa nº 1.888 de 2019²⁰⁵, que instituiu e disciplinou a obrigatoriedade da prestação de informações relativas às operações realizadas com criptoativos à Secretaria Especial da Receita Federal do Brasil (RFB). Nessa, foram estabelecidos alguns conceitos importantes como a definição jurídica, para a RFB, do que seria um criptoativo, como já mencionado no capítulo anterior, bem como o que seria uma *Exchange* de criptoativo.

204 “A maioria das corretoras tem uma carteira quente para os saques do dia-a-dia e outra em armazenamento frio com o grosso dos fundos depositados, recarregando uma em função da outra de acordo com suas políticas de gestão de riscos” **Glossário ABCRIPTO**. Versão 1.1, 03 jul. 2023. fl.3 Disponível em: https://backend.abcripto.com.br/media/files/documentsDownloadSection/glossario_abcripto_v1.pdf Acesso em 16.ou.2025

205 **RECEITA FEDERAL DO BRASIL**. Instrução Normativa RFB nº 1888, de 3 de maio de 2019. Institui e disciplina a obrigatoriedade de prestação de informações relativas às operações realizadas com criptoativos à Secretaria Especial da Receita Federal do Brasil (RFB). Disponível em: <https://normasinternet2.receita.fazenda.gov.br/#/consulta/externa/100592/visao/multivigente>. Acesso em: 16 out. 2025.

Art. 5º Para fins do disposto nesta Instrução Normativa, considera-se: (...)

II - exchange de criptoativo: a pessoa jurídica, ainda que não financeira, que oferece serviços referentes a operações realizadas com criptoativos, inclusive intermediação, negociação ou custódia, e que pode aceitar quaisquer meios de pagamento, inclusive outros criptoativos.

Parágrafo único. Incluem-se no conceito de intermediação de operações realizadas com criptoativos, a disponibilização de ambientes para a realização das operações de compra e venda de criptoativo realizadas entre os próprios usuários de seus serviços²⁰⁶.

Posteriormente, a Instrução Normativa nº 1.899, também de 2019, trouxe aperfeiçoamentos técnicos e procedimentos complementares para fortalecer a atuação da Receita Federal nesse âmbito.

8. COMISSÃO DE VALORES MOBILIÁRIOS (CVM)

Em 2022, a CVM publicou a Resolução CVM nº 88, revogando a Instrução CVM nº 588, ampliando a possibilidade de ofertas públicas de valores mobiliários para empresas de pequeno porte, através de plataformas de investimento coletivo, chamadas de plataformas de *crowdfunding* de investimento²⁰⁷.

Apesar dessa resolução não ter tratado especificamente sobre criptoativos, representou um marco importante para o desenvolvimento do ecossistema de *tokens* no Brasil, especialmente ao fornecer as bases regulatórias que viabilizaram a utilização da

206 Art. 5º, inciso II e parágrafo único. **BRASIL. Receita Federal do Brasil.** Instrução Normativa RFB nº 1.888, de 3 de maio de 2019. Art. 5º, inciso II e parágrafo único. Disponível em: <https://normasinternet2.receita.fazenda.gov.br/#/consulta/externa/100592/visao/multivigente>. Acesso em: 16 out. 2025.

207 **CVM.** Resolução CVM nº 88, de 2022. Dispõe sobre a oferta pública de distribuição de valores mobiliários de emissão de sociedades empresárias de pequeno porte realizada com dispensa de registro por meio de plataforma eletrônica de investimento participativo e revoga a Instrução CVM nº 588, de 13 de julho de 2017. Disponível em: <https://conteudo.cvm.gov.br/legislacao/resolucoes/resol088.html>. Acesso em: 16 out. 2025.

tecnologia de registros distribuídos, como a *blockchain*, na emissão e oferta pública de valores mobiliários por pequenas e médias empresas. Seu impacto mais relevante se deu ao permitir, de forma implícita, que os valores mobiliários ofertados por meio das plataformas de investimento participativo pudessem ser representados digitalmente, inclusive sob a forma de *tokens*.

Com a Resolução CVM nº 88, criou-se um ambiente jurídico seguro e estruturado para a atuação de plataformas digitais de captação de recursos, abrindo espaço para a adoção da tokenização como uma tecnologia aplicável à emissão e distribuição de ativos. A norma, ao não restringir a forma de representação dos valores mobiliários ofertados, foi interpretada como tecnologicamente neutra e – portanto - apta a abarcar diferentes formas de emissão e registro, incluindo aquelas baseadas em DLT. Dessa forma, passou a ser possível estruturar ofertas públicas em que os valores mobiliários fossem emitidos na forma de *tokens*, respeitados os requisitos e limites estabelecidos pela própria Resolução.

Além disso, a Resolução nº 88 estimulou o ingresso de novas plataformas no mercado, muitas das quais voltadas especificamente à tokenização de ativos. Essas plataformas passaram a se registrar junto à CVM e a operar sob sua supervisão. A consequência foi uma ampliação das possibilidades de captação para emissores de menor porte e o fortalecimento da infraestrutura necessária para que a tokenização se consolidasse como uma ferramenta legítima e compatível com o ordenamento jurídico brasileiro²⁰⁸.

208 “O cenário regulatório, contudo, mudou substancialmente após a edição dos Ofícios-Circulares SSE 04/2023 e 06/2023 (em conjunto, “Ofícios-Circulares”), que reconheceram a possibilidade de oferta, via crowdfunding, de *tokens* representativos de certificados de recebíveis e de outros títulos de securitização emitidos por companhias securitizadoras de capital fechado. Desde então, observou-se crescimento expressivo nas ofertas e volumes captados - de R\$ 220 milhões em 2023 para R\$ 1,5 bilhão em 2024, sendo 70% das ofertas (227 de 323) e 76% do volume relacionados a certificados de recebíveis.” **CVM**. Edital de Consulta Pública SDM nº 05/25. fl. 1. Disponível em: https://conteudo.cvm.gov.br/audiencias_publicas/ap_sdm/2025/sdm0525.html. Acesso em: 16 out. 2025.

É importante destacar que os efeitos da Resolução nº 88 foram posteriormente reforçados pelo Parecer de Orientação CVM nº 40, publicado em outubro de 2022, que trouxe – como já abordado – diretrizes interpretativas sobre a natureza jurídica dos criptoativos e seus possíveis enquadramentos como valores mobiliários. O parecer esclareceu que determinados *tokens*, podem configurar valores mobiliários nos termos da Lei nº 6.385/1976, estando, portanto, sujeitos à supervisão da CVM. Nesse sentido, destaca-se o entendimento da CVM no parecer de orientação 40 e em consonância com a Lei 6.385/76 e a Lei nº 10.303/01.

Parecer de orientação 40:

Ainda que os criptoativos não estejam expressamente incluídos entre os valores mobiliários citados nos incisos do art. 2º da Lei nº 6.385/76, os agentes de mercado **devem analisar as características de cada criptoativo** com o objetivo de determinar se é valor mobiliário, o que ocorre quando:

(I) é a **representação digital** de algum dos valores mobiliários previstos taxativamente nos incisos I a VIII do art. 2º da Lei nº 6.385/76 e/ou previstos na Lei nº 14.430/2022 (i.e., certificados de recebíveis em geral); ou

(II) enquadra-se no conceito aberto de valor mobiliário do inciso IX do art. 2º da Lei nº 6.385/76, na medida em que seja contrato de investimento coletivo²⁰⁹.

Lei nº 6.385/76 e Lei nº 10.303/01:

Art. 2o São valores mobiliários sujeitos ao regime desta Lei:

(Redação dada pela Lei nº 10.303, de 31.10.2001)

I - as ações, debêntures e bônus de subscrição;

(Redação dada pela Lei nº 10.303, de 31.10.2001)

209 **CVM.** Parecer de Orientação nº 40, de 11 de outubro de 2022. fl. 6. Disponível em: <https://conteudo.cvm.gov.br/legislacao/pareceres-orientacao/pare040.html>. Acesso em: 16 out. 2025.

II - os cupons, direitos, recibos de subscrição e certificados de desdobramento relativos aos valores mobiliários referidos no inciso II;

(Redação dada pela Lei nº 10.303, de 31.10.2001)

III - os certificados de depósito de valores mobiliários;

(Redação dada pela Lei nº 10.303, de 31.10.2001)

IV - as cédulas de debêntures;

(Inciso incluído pela Lei nº 10.303, de 31.10.2001)

V - as cotas de fundos de investimento em valores mobiliários ou de clubes de investimento em quaisquer ativos;

(Inciso incluído pela Lei nº 10.303, de 31.10.2001)

VI - as notas comerciais;

(Inciso incluído pela Lei nº 10.303, de 31.10.2001)

VII - os contratos futuros, de opções e outros derivativos, cujos ativos subjacentes sejam valores mobiliários;

(Inciso incluído pela Lei nº 10.303, de 31.10.2001)

VIII - outros contratos derivativos, independentemente dos ativos subjacentes; e

IX - quando ofertados publicamente, quaisquer outros títulos ou contratos de investimento coletivo, que gerem direito de participação, de parceria ou de remuneração, inclusive resultante de prestação de serviços, cujos rendimentos advêm do esforço do empreendedor ou de terceiros²¹⁰. (grifo nosso)

A interpretação conjunta desses normativos consolidou o entendimento de que os *tokens* podem, sim, ser utilizados como meios de representação de valores mobiliários, desde que observadas as normas vigentes. Nesse sentido, a Resolução CVM nº 88 teve o papel fundamental de operacionalizar, na prática, a emissão desses ativos

210 **BRASIL.** Lei nº 6.385, de 7 de dezembro de 1976. Dispõe sobre a constituição e funcionamento da Comissão de Valores Mobiliários (CVM). Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l6385.htm. Acesso em: 16 out. 2025. e **BRASIL.** Lei nº 10.303, de 31 de outubro de 2001. Altera dispositivos da Lei nº 6.385/76, que dispõe sobre a constituição e funcionamento da CVM. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/LEIS_2001/L10303.htm#art1. Acesso em: 16 out. 2025.

digitais por meio de plataformas reguladas, assegurando que as ofertas realizadas nesse formato estejam inseridas no escopo da proteção regulatória conferida aos investidores.

A CVM continuou aprimorando sua orientação regulatória sobre criptoativos por meio da publicação, em 2023, dos Ofícios Circulares SSE nº 4²¹¹ e nº 6²¹². Esses documentos aprofundaram a caracterização de *tokens* de recebíveis ou *tokens* de renda fixa (TR) como valores mobiliários e esclareceram que esses devem observar as normas da CVM. Os ofícios reforçaram ainda que a ausência de manifestação prévia da autarquia não exime os emissores do cumprimento das obrigações legais e regulatórias aplicáveis. Em 2025, o Ofício Circular SSE nº 4 complementou essa linha de atuação, detalhando as obrigações das plataformas de *crowdfunding* em face da Resolução CVM nº 88²¹³.

Por fim, embora a Resolução CVM nº 88 tenha sido suficiente para permitir a tokenização de valores mobiliários em ofertas públicas de pequeno porte, a sua aplicação prática revelou desafios que ainda demandam aprimoramentos normativos. Dentre esses desafios, destacam-se a ausência de previsão expressa sobre a tokenização, a falta de regulamentação específica para o mercado secundário de negociação desses ativos e questões relacionadas à custódia, liquidação e interoperabilidade entre plataformas. Tais lacunas motivaram a Comissão de Valores Mobiliários a abrir, em setembro de

211 “Este Ofício Circular tem o propósito de orientar os prestadores de serviços envolvidos na atividade de tokenização sobre a provável natureza de valor mobiliário dos chamados “*Tokens* de Recebíveis” ou “*Tokens* de Renda Fixa” (em conjunto “TR”), seja nos termos do art. 2º, inciso IX, da Lei nº 6.385, de 7 de dezembro de 1976, ou dos arts. 18, parágrafo único, e 19, da Lei nº 14.430, de 3 de agosto de 2022.” **CVM** Ofício-Circular nº 4/2023/CVM/SSE - Disponível em: <https://conteudo.cvm.gov.br/legislacao/oficios-circulares/sse1/oc-sse-0423.html> Acesso em 16.out.2025

212 “O presente Ofício Circular tem como objetivo complementar as manifestações desta Superintendência de Supervisão de Securitização (SSE), contidas no Ofício Circular nº 4/2023-CVM/SSE (“OC 4/23”), acerca dos denominados *tokens* de recebíveis ou *tokens* renda fixa (em conjunto “TR”). **CVM** Ofício-Circular nº 6/2023/CVM/SSE. Disponível em: <https://conteudo.cvm.gov.br/export/sites/cvm/legislacao/oficios-circulares/sse1/anexos/oc-sse-0623.pdf> Acesso em 16.out.2025

213 “Orientações gerais às plataformas sobre o cumprimento de dispositivos da Resolução CVM nº 88 (“RCVM 88”). Disponível em: <https://conteudo.cvm.gov.br/legislacao/oficios-circulares/sse1/oc-sse-0425.html> Acesso em 16.out.2025

2025, uma consulta pública com o objetivo de revisar a RCVN nº88²¹⁴. No momento da finalização desse trabalho, essa consulta ainda está em fase de considerações.

Ainda sobre o Parecer de Orientação nº 40, cabe sinalizar que esse se tornou referência para o enquadramento jurídico dos criptoativos sob a perspectiva da regulação do mercado de capitais, visto que esse estabeleceu uma categorização clara dos ativos digitais em *tokens* de pagamento, *tokens* de utilidade e *tokens* referenciados a ativos, ressaltando que nem todo criptoativo configura valor mobiliário, cabendo à análise detalhada da estrutura e finalidade do ativo digital essa definição.

9. LEGISLATIVO E O BANCO CENTRAL

No âmbito legislativo, o ano de 2022 também foi palco da aprovação da Lei nº 14.478²¹⁵, o chamado Marco Legal das Criptomoedas, que representou o primeiro esforço legislativo nacional para estabelecer definições, diretrizes e responsabilidades relacionadas ao mercado de ativos virtuais. Essa lei definiu os conceitos de ativo virtual e de prestador de serviço de ativo virtual (PSAV), proibiu o uso desses ativos como moeda de curso forçado e instituiu mecanismos de responsabilização para fraudes e ilícitos praticados com criptoativos. Ademais, a legislação conferiu ao Poder Executivo a prerrogativa de indicar o órgão regulador do setor, atribuição esta que, posteriormente, recaiu sobre o Banco Central do Brasil, por meio do Decreto nº 11.563, de 2023.

214 “Reforma da Resolução CVM nº 88, de 27 de abril de 2022, que dispõe sobre a oferta pública de distribuição de valores mobiliários de emissão de sociedades empresárias de pequeno porte realizada com dispensa de registro por meio de plataforma eletrônica de investimento participativo.” **CVM**. EDITAL DE CONSULTA PÚBLICA SDM Nº 05/25. Disponível em: https://conteudo.cvm.gov.br/audiencias_publicas/ap_sdm/2025/sdm0525.html Acesso em 16.out.2025

215 **BRASIL**. LEI Nº 14.478, DE 21 DE DEZEMBRO DE 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/lei/l14478.htm Acesso em 16.out.2025

DECRETO Nº 11.563, DE 13 DE JUNHO DE 2023

(...)

DECRETA:

Art. 1º Este Decreto regulamenta a Lei nº 14.478, de 21 de dezembro de 2022, para estabelecer ao Banco Central do Brasil competência para:

I - regular a prestação de serviços de ativos virtuais, observadas as diretrizes da referida Lei;

II - regular, autorizar e supervisionar as prestadoras de serviços de ativos virtuais; e

III - deliberar sobre as demais hipóteses estabelecidas na Lei nº 14.478, de 2022, ressalvado o disposto no art. 12, na parte que inclui o art. 12-A na Lei nº 9.613, de 3 de março de 1998²¹⁶ (grifo nosso).

A partir dessa designação, o Banco Central iniciou um amplo processo normativo que culminou na publicação, em 2024, das Consultas Públicas nº 109, 110 e 111. Essas consultas trataram, respectivamente, da regulamentação das PSAVs, do processo de autorização para atuação dessas instituições, e das operações envolvendo criptoativos no mercado de câmbio. Tais consultas foram bem-vistas pelos diferentes *players* do mercado. Associações, *exchanges* e até pessoas físicas se manifestaram.

6. BREVE RESUMO SOBRE PENHORA

A penhora é, em essência, um ato jurídico de apreensão de bens, decorrente de decisão judicial, que tem como finalidade a satisfação de crédito em sede de execução. Nesse sentido, o Exmo. Professor Desembargador Alexandre Câmara conceitua a penhora como:

(...) o ato de apreensão judicial dos bens que serão empregados, direta, ou indiretamente, na satisfação do crédito exequendo. Em

²¹⁶ Art. 1º, inciso I, II e III . **BRASIL**. DECRETO Nº 11.563, DE 13 DE JUNHO DE 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11563.htm Acesso em 15.out.2025

outras palavras, a penhora é um ato de constrição patrimonial, através do qual são apreendidos bens que serão utilizados como meio destinado a viabilizar a realização do crédito do exequente²¹⁷.

De forma mais sucinta, o eminente Professor José Carlos Barbosa Moreira define a penhora como sendo: *“o ato pelo qual se apreendem bens para empregá-los, de maneira direta ou indireta, na satisfação do crédito exequendo.”*²¹⁸

A partir dessas definições, é possível distinguir duas modalidades de satisfação do crédito: direta e indireta. A satisfação direta ocorre quando o próprio bem penhorado é utilizado para quitar a obrigação, consubstanciada em título executivo certo, líquido e exigível, hipótese que, geralmente, se concretiza mediante adjudicação judicial. Por sua vez, a satisfação indireta dá-se quando o bem penhorado é convertido em pecúnia, sendo o valor arrecadado destinado ao exequente para adimplemento da obrigação²¹⁹.

Ainda com base nas lições do Professor e Desembargador Alexandre Câmara, a penhora produz cinco efeitos, os quais se dividem em duas naturezas: três de ordem processual e dois de ordem material, também denominada substancial.

217 **CÂMARA**, Alexandre F. O Novo Processo Civil Brasileiro - 8ª Edição 2022. 8. ed. Rio de Janeiro: Atlas, 2022. E-book. p.397. ISBN 9786559772575. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9786559772575/> Acesso em: 16 out. 2025.

218 **MOREIRA**, José Carlos B. O Novo Processo Civil Brasileiro - 29ª Edição 2012. Rio de Janeiro: Forense, 2012. E-book. p.237. ISBN 978-85-309-4385-1. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/978-85-309-4385-1/>. Acesso em: 16 out. 2025.

219 Penhora é o ato de apreensão judicial dos bens que serão empregados, direta ou indiretamente, na satisfação do crédito exequendo. Em outras palavras, a penhora é um ato de constrição patrimonial, através do qual são apreendidos bens que serão utilizados como meio destinado a viabilizar a realização do crédito do exequente. Esta utilização pode ser direta (que se dá quando o próprio bem apreendido é entregue ao exequente a título de pagamento da dívida, por intermédio de uma técnica de expropriação chamada adjudicação) ou indireta (que ocorre nos casos em que o bem penhorado é expropriado e transformado em dinheiro, usando-se esta verba, obtida com a alienação do bem penhorado, para pagar o credor). **CÂMARA**, Alexandre F. **O Novo Processo Civil Brasileiro** - 8ª Edição 2022. 8. ed. Rio de Janeiro: Atlas, 2022. E-book. p.397. ISBN 9786559772575. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9786559772575/>. Acesso em: 16 out. 2025.

No que se refere aos efeitos processuais, o primeiro consiste em estabelecer uma garantia em juízo, conferindo efetividade à execução e assegurando a obtenção do resultado prático almejado. O segundo efeito é a individualização dos bens atingidos pela execução, delimitando o patrimônio submetido à constrição judicial. O terceiro é a instituição do direito de preferência, aplicável nos casos em que houver pluralidade de credores.

Quanto aos efeitos materiais ou substanciais, destaca-se, primeiramente, a perda da posse direta do bem penhorado. Conforme explica o professor e Des. Câmara, ocorre o chamado desdobramento forçado da posse, pelo qual o Estado passa a deter a posse direta do bem objeto da penhora, enquanto o executado conserva a posse indireta, como no caso da penhora de bem imóvel, em que o devedor permanece na posse e propriedade formal do bem até ulterior deliberação judicial. O segundo efeito de natureza material é a ineficácia dos atos de alienação ou oneração do bem realizados pelo executado após a efetivação da penhora²²⁰.

10. A PENHORA DE CRIPTOATIVOS NO BRASIL

Como já sinalizado, a expansão do uso de criptoativos no Brasil trouxe à tona desafios práticos e jurídicos ainda não completamente enfrentados pelo sistema de justiça, em especial no que se refere à efetivação da penhora desses bens nos processos de execução. Atualmente, no Brasil, a constrição judicial de criptoativos tem se dado, de forma majoritária, por meio da expedição de ofícios judiciais direcionados às *exchanges* requerendo a indisponibilização de ativos vinculados ao CPF ou CNPJ do executado. Nesse sentido, cabe aludir a recente decisão do STJ:

220 **CÂMARA**, Alexandre F. O Novo Processo Civil Brasileiro - 8ª Edição 2022. 8. ed. Rio de Janeiro: Atlas, 2022. E-book. p.397. ISBN 9786559772575. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9786559772575/>. Acesso em: 16 out. 2025.

RECURSO ESPECIAL Nº 2127038 - SP (2024/0066151-9)

(...)

3. Registre-se que a Instrução Normativa da Receita Federal do Brasil – IN RFB n. 1.888/2019 institui e disciplina a obrigatoriedade de prestação de informações relativas às operações realizadas com criptoativos à Secretaria Especial da Receita Federal do Brasil.

4. Trata-se de um ativo financeiro passível de tributação, cujas operações devem ser declaradas à Receita Federal, sendo, portanto, um bem de valor econômico, suscetível de eventual constrição. Apesar de não serem moeda de curso legal, os criptoativos podem ser usados como forma de pagamento e como reserva de valor.

5. Em observância aos princípios que norteiam o processo de execução e o interesse das partes credora e devedora, é plenamente possível a expedição de ofício às corretoras de criptomoedas (exchanges) ou a utilização de medidas investigativas para acessar as carteiras digitais do devedor, tal qual pleiteado pela parte credora para eventual penhora²²¹. (grifo nosso)

Esse envio de ofícios é um procedimento moroso e, muitas vezes, ineficaz, uma vez que sua viabilidade depende de conhecimento prévio sobre qual plataforma o devedor utiliza e se os ativos estão, de fato, sob custódia de uma corretora centralizada. Caso os criptoativos estejam em regime de auto-custódia ou em corretoras descentralizadas (DEXs), não há a quem se dirigir, tampouco há meios técnicos diretos para bloqueá-los, tornando ineficaz a determinação judicial.

Além disso, mesmo diante da identificação de corretoras tradicionais, não há um sistema unificado ou automatizado de comunicação entre o Poder Judiciário e essas plataformas, o que torna

221 **BRASIL**. Superior Tribunal de Justiça. Recurso Especial nº 2127038-SP (2024/0066151-9). Relator: Ministro Humberto Martins. Recorrente: Pearson Education do Brasil Ltda. Recorrido: Ubiratan Rios Lima. Brasília, DF, julgado em 18 de fevereiro de 2025. Disponível em: <https://processo.stj.jus.br/processo/pesquisa/?aplicacao=processos.ea&tipoPesquisa=tipoPesquisaGenerica&termo=REsp%202127038> Acesso em: 16.out.2025

o processo lento, sujeito a falhas de tramitação, atrasos e respostas incompletas decorrentes de dúvidas práticas.

Outro entrave operacional importante reside na ausência de uma normatização padronizada quanto à forma como as corretoras devem atender às ordens judiciais. Cada *exchange* adota seus próprios critérios internos, o que resulta em respostas distintas para ofícios semelhantes. Há casos em que as plataformas solicitam informações adicionais, exigem formalidades cartorárias ou simplesmente não respondem aos pedidos. Tal cenário compromete a previsibilidade e a efetividade da tutela jurisdicional, especialmente em execuções que dependem da celeridade na constrição patrimonial.

Também se observa a dificuldade de verificação de autenticidade e suficiência dos ativos eventualmente bloqueados. Ao contrário do sistema bancário tradicional, que conta com plataformas como o SISBAJUD, que permite bloqueio, rastreo e levantamento automático de valores em contas e que possui uma regulamentação própria pelo CNJ²²², o Judiciário brasileiro ainda não dispõe de um sistema similar voltado aos criptoativos, o que amplia a vulnerabilidade das execuções diante de um cenário digital descentralizado.

Além das questões técnicas e procedimentais, é fundamental destacar os problemas jurisdicionais decorrentes da natureza globalizada das *exchanges* de criptoativos. Algumas corretoras possuem sede no exterior e, frequentemente, não mantêm representação jurídica no Brasil, nem estabelecem domicílio jurídico no país. Isso dificulta ou até inviabiliza o cumprimento de ordens judiciais expedidas por autoridades brasileiras, seja por ausência de cooperação internacional formal, seja pela própria falta de normatização sobre obrigações dessas plataformas diante de determinações do Judiciário nacional.

222 **CNJ.** portaria Nº SEP 2/2025 de 04 de agosto de 2025. Altera o Anexo da Portaria SEP n. 3/2024, que regula o uso e o funcionamento do Sistema de Busca de Ativos do Poder Judiciário – Sisbajud. Disponível em: <https://atos.cnj.jus.br/files/original200313202508066893b50119290.pdf> . Acesso em 16.out.2025

Mesmo aquelas que atuam no mercado brasileiro, o que pode ser notado através da tradução dos seus sites para o português, oferecendo atendimento local e aceitando depósitos em reais, muitas vezes o fazem sem submissão expressa à jurisdição brasileira, valendo-se de cláusulas contratuais que elegem foro estrangeiro ou que não preveem qualquer mecanismo de cooperação com o sistema judicial nacional. Esse fator acirra a insegurança jurídica e compromete a efetividade da execução, principalmente em casos urgentes ou em que o executado se vale da internacionalização dos ativos para frustrar a atividade jurisdicional.

Diante dessas limitações, foi percebido pelas mais diferentes entidades, a necessidade de um método padronizado, célere e tecnicamente adequado para a penhora de criptoativos. Nesse contexto, ganha destaque a proposta de criação do Sistema Criptojud, concebido como uma ferramenta especializada de comunicação entre o Poder Judiciário e os principais agentes do mercado de criptoativos.

A iniciativa visa permitir a consulta, rastreamento e bloqueio automatizado de ativos digitais, a exemplo do que já ocorre com valores em instituições financeiras por meio do Sisbajud. O detalhamento do funcionamento proposto para o Criptojud, bem como os desafios jurídicos e técnicos que sua implementação levanta, será objeto de análise no capítulo seguinte.

11. CRIPTOJUD

Com o reconhecimento crescente de que os criptoativos integram o patrimônio dos devedores e são passíveis de constrição judicial, revelam-se insuficientes os meios tradicionais de ofício judicial para corretoras, dadas as limitações operacionais, jurisdicionais e tecnológicas. Para superar essas deficiências, foi lançada a proposta de implementação do Sistema Criptojud, iniciativa liderada pelo

Conselho Nacional de Justiça (CNJ) com vistas a modernizar e tornar mais efetiva a penhora de ativos digitais no Brasil²²³.

O Criptojud pretende funcionar como uma plataforma integrada ao ecossistema digital do Poder Judiciário, permitindo que juízes, varas e tribunais acessem de forma padronizada e automatizada os dados de custódia de criptoativos mantidos por *exchanges* que aderirem ao sistema. Na primeira fase, o sistema deverá possibilitar localização e bloqueio de ativos digitais, mediante envio automático de ordens judiciais padronizadas as *exchanges* que tiverem aderido ao sistema. Em fases posteriores, está previsto que o Criptojud também permita a transferência dos ativos para contas judiciais sob guarda institucional e, eventualmente, a liquidação financeira em moeda nacional, convertendo as criptomoedas penhoradas em reais ou valores equivalentes²²⁴.

Porém, a efetividade do Criptojud dependerá de alguns fatores, dentre os quais a custódia em uma Exchange regulada. Nos casos que o ativo está em auto-custódia, em carteiras offline ou em plataformas descentralizadas, não haverá agente institucional a ser solicitado para cumprir ordens judiciais²²⁵.

223 CNJ. **CriptoJud: novo sistema possibilita consulta on-line da posse de criptoativos por devedores.** Disponível em: <https://www.cnj.jus.br/criptojud-novo-sistema-possibilita-consulta-on-line-da-posse-de-criptoativos-por-devedores/>. Acesso em 16.out.2025

224 “Desenvolvido em parceria com a Associação Brasileira de Criptoeconomia (Abcripto), o CriptoJud será implementado em tribunais de todo o país por meio do Portal Jus.br, conforme cronograma a ser divulgado em 12 de agosto. O sistema estará integrado à Plataforma Digital do Poder Judiciário (PDPJBr) e seguirá os mais altos padrões de segurança cibernética. Além de permitir o bloqueio automático de criptomoedas, o sistema também prevê, em fases futuras, a custódia em contas judiciais e a liquidação dos valores em moeda nacional, ampliando a efetividade das decisões judiciais.” Portal do Bicoín. **CriptoJud: Novo sistema da Justiça vai facilitar bloqueio de criptomoedas em exchanges.** Novo sistema possibilita consulta on-line da posse de criptomoedas por devedores em processos judiciais. Disponível em: <https://portaldobitcoin.uol.com.br/criptojud-novo-sistema-da-justica-vai-facilitar-bloqueio-de-criptomoedas-em-exchanges/> Acesso em 16.out.2025

225 “O alcance do CriptoJud deverá ter, ainda assim, limitações, segundo explicam os especialistas. Isso se deve ao fato de que os criptoativos não precisam necessariamente estar custodiados nas corretoras online.” **OAM ADVOGADOS.** *Criptojud deve agilizar penhora de criptoativos.* Disponível em: <https://www.oam.adv.br/2024/11/criptojud->

Ademais, surgem desafios jurídicos centrais: pode-se exigir normativa que obrigue as exchanges a participarem do sistema, ou prever sanções para quem se recusar; será necessário regulamentar o fluxo de dados pessoais e sensíveis relacionados aos clientes dessas plataformas e conciliar a transparência judicial com a proteção de dados e sigilo financeiro. Deve-se também contemplar mecanismos para garantir o contraditório e a ampla defesa, evitando arbitrariedades no bloqueio ou na transferência de ativos.

Nesse sentido, cabe observar que há um projeto de lei 1600/22 que busca, entre outros diversos pontos, acrescentar criptoativos ao Art. 835 do CPC, que versa sobre penhora:

Art. 835. A penhora observará, preferencialmente, a seguinte ordem: (...)

XIV – **criptoativos**, assim entendidos como representações digitais de valor que, não sendo moeda, possuam unidade de medida própria, negociados eletronicamente por meio da utilização de criptografia e no âmbito de tecnologias de registro distribuído, utilizados como ativo financeiro, meio de troca ou pagamento, instrumento de acesso a bens e serviços ou investimento. (grifo nosso)

Em termos técnicos, o Criptojud precisará definir protocolos seguros e auditáveis de comunicação com sistemas das exchanges, lidar com diferentes *blockchains*, padrões de *tokens* e formatos de carteira, bem como garantir a interoperabilidade entre diversas redes e sistemas de custódia. Outro ponto crítico é a liquidação: converter ativos digitais voláteis em moeda fiduciária exigirá infraestrutura, prazos e mecanismos de arbitragem e garantia de valor.

12. VIABILIDADE DO CRIPTOJUD

A implementação do Criptojud não está isenta de desafios jurídicos, técnicos e operacionais, os quais merecem análise cautelosa

deve-agilizar-penhora-de-criptoativos-mas-nao-evita-fraudes/. Acesso em: 16 out. 2025.

para que o sistema alcance seus objetivos sem gerar insegurança ou violações a direitos fundamentais.

Um dos pontos centrais de dificuldades na implementação do Criptojud estava no fato que boa parte das *exchanges* com atuação no Brasil não possuíam nenhum tipo de representação formal ou sede no território nacional, o que impactava diretamente no recebimento desses ofícios e – no limite – na efetividade do seu cumprimento, por uma questão jurisdicional. No entanto, no dia 10 de novembro de 2025, algumas resoluções do Banco Central foram publicadas – decorrentes das consultas públicas 109, 110, 111 do BACEN.

Essas resoluções mudam completamente a análise da viabilidade do Criptojud, de forma que se torna imperativa a necessidade de análise da possibilidade de penhora através dessas novas disposições.

13. NOVAS RESOLUÇÕES DO BANCO CENTRAL E O IMPACTO DIRETO NO MUNDO DA PENHORA

Em 10 de novembro de 2025 o Banco Central publicou as resoluções decorrentes das mencionadas consultas públicas. A Resolução 519 disciplina como se dará o processo de autorização para o funcionamento das Sociedades Prestadoras de Serviços de Ativos Virtuais (SPSAVs), bem como sobre como o processo de autorização para que algumas instituições já abarcadas pelo CMN possam requerer prestar esse tipo de serviço, tornando-se uma Prestadora de Serviços de Ativos Virtuais (PSAVs). De forma clara, as SPSAVs e as PSAVs tornam-se, efetivamente, parte do cenário financeiro nacional, estando oficialmente reguladas pelo Banco Central.

Já a Resolução 520 – a mais detalhada dentro desse grupo de resoluções – disciplina como se dará a prestação desse serviço, quem poderá prestá-lo e como será a constituição e o funcionamento das SPSAVs. Essa resolução representou um grande avanço regulatório, pontuando – inclusive – diferenças entre conceitos como: custodiante, intermediária e corretora de ativos virtuais. Nesse sentido:

CAPÍTULO IV

DAS MODALIDADES DE PRESTADORAS DE SERVIÇOS DE ATIVOS VIRTUAIS

Art. 4º As sociedades prestadoras de serviços de ativos virtuais são instituições autorizadas a funcionar pelo Banco Central do Brasil que executam, em nome de terceiros, a prestação de serviços de ativos virtuais nas modalidades previstas nesta Resolução.

§ 1º As sociedades de que trata o caput são classificadas nas seguintes modalidades, de acordo com os serviços de ativos virtuais prestados:

I - intermediárias de ativos virtuais;

II - custodiantes de ativos virtuais; e

III - corretoras de ativos virtuais.

§ 2º É vedado às sociedades prestadoras de serviços de ativos virtuais de que trata o § 1º, incisos I e II, a execução combinada de atividades de outras modalidades de sociedades prestadoras de serviços de ativos virtuais.

Art. 5º As sociedades prestadoras de serviços de ativos virtuais somente podem exercer as atividades expressamente previstas nesta Resolução e nos demais regulamentos em vigor.

A resolução discorre sobre cada uma das funções de cada um desses agentes, o que impacta – por exemplo – no entendimento de envio de uma eventual ordem judicial de penhora de criptoativos. Sendo necessário compreender – por exemplo – se o ativo está em uma corretora – que cumula a função de custodiante com intermediária²²⁶ – ou em uma custodiante “pura”.

Além disso, abarcou esses diferentes *players* de mercado dentro do escopo regulatório do BACEN, apontando novas exigibilidades

226 **BANCO CENTRAL DO BRASIL.** Das corretoras de ativos virtuais Art. 10. As corretoras de ativos virtuais têm por objeto social a intermediação e a custódia de ativos virtuais. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/exibennormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=520> Acesso em 22.nov.2025

como: requisitos de governança, segurança, controles internos e prestação de informações.

Um dos pontos de destaque é que de acordo com a Resolução BCB nº 520 as SPSAVs e as PSAVs deverão estar constituídas no Brasil e possuir sede e administração localizadas em território nacional²²⁷, o que também impacta diretamente na efetividade de sistemas como o Criptojud. Se, anteriormente, uma das grandes questões sobre a efetividade desse sistema estava voltado para o fato que muitas Exchanges estavam fora do território nacional e não possuíam representação, nesse novo cenário, há necessidade clara de que as PSAVs e as SPSAVs estejam dentro do arcabouço regulatório nacional, não só com sede física, mas com representação frente ao Banco Central, uma vez que para SPSAVs sejam constituídas será preciso possuir pelo menos três diretores ou administradores responsáveis perante o Banco Central do Brasil²²⁸.

Além disso, a Resolução prevê inúmeros pontos voltados para governança e comunicação com o BACEN por meio do Cadastro de Clientes do Sistema Financeiro Nacional (CCS) sobre características contábeis e cadastrais.

Art. 87. Além dos regulamentos e disciplinas mencionados nesta Resolução, **as sociedades prestadoras de serviços de ativos virtuais** devem observar o conjunto da regulamentação estabelecida para as

227 **BANCO CENTRAL DO BRASIL.** Resolução BCB nº 520 de 10/11/2025. Art. 1º Esta Resolução disciplina a constituição e o funcionamento das sociedades prestadoras de serviços de ativos virtuais e a prestação de serviços de ativos virtuais por outras instituições autorizadas a funcionar pelo Banco Central do Brasil. Parágrafo único. Para os fins do disposto no caput, o funcionamento das prestadoras de serviços de ativos virtuais no país é caracterizado se a prestadora: I - está constituída no Brasil, nos termos da legislação e da regulamentação aplicáveis; e II - possui sede e administração localizadas em território nacional e submetidas ao ordenamento jurídico e às autoridades do Brasil. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/exibennormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=520> Acesso em 22.nov.2025

228 **BANCO CENTRAL DO BRASIL.** Resolução BCB nº 520 de 10/11/2025. Art. 14. A sociedade prestadora de serviços de ativos virtuais deve: (...) III - possuir pelo menos três diretores ou administradores responsáveis perante o Banco Central do Brasil pelo cumprimento da regulamentação relativa: Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/exibennormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=520> Acesso em 22.nov.2025

instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil, conforme aplicáveis.

Art. 88. As sociedades que, na data da entrada em vigor desta Resolução, estiverem realizando uma ou mais das atividades indicadas no art. 7º, caput e incisos, e no art. 9º, caput e incisos, devem:

III - enviar, **a partir** do protocolo do pedido de autorização de que trata o inciso I até a conclusão da fase 1 do processo de autorização para funcionamento, na forma das regulamentações específicas:

a) informações relativas aos seus clientes e usuários, ou representantes legais ou convencionais desses clientes ou usuários, ao **Cadastro de Clientes do Sistema Financeiro Nacional;**

b) **diariamente, as informações e os dados relativos aos saldos contábeis mantidos pela instituição em favor de seus clientes e usuários, nos termos da regulamentação específica;**

c) **diariamente, as informações e os dados relativos à prestação de serviços de custódia de ativos virtuais, equivalentes ao total de ativos virtuais custodiados, por conta própria ou de terceiros, no país ou no exterior, informados por quantidades e pelos respectivos valores financeiros, bem como as quantidades totais e valores agregados custodiados em favor de cada cliente ou usuário;**

d) **mensalmente, demonstrações verificáveis, na forma de provas de reservas de ativos virtuais mantidos, discriminadas por ativo virtual, em relação às quantidades e aos valores financeiros custodiados desses ativos virtuais para seus clientes ou usuários;**

e) **mensalmente, demonstrações verificáveis, contendo o total de ativos virtuais de clientes ou usuários que estejam destinados às operações de staking, caso a instituição realize essas operações; e**

f) **tempestivamente, as informações e os documentos que o Banco Central do Brasil vier a requisitar, complementarmente, no âmbito de sua competência legal de autorização, monitoramento e supervisão (grifo nosso).**

Um ponto que cabe menção é que o SISBAJUD, que é o sistema utilizado pelo judiciário para realizar o envio do pedido de bloqueio, desbloqueio e transferência de ativos financeiros para Instituições Financeiras, se comunica à IF através do sistema CCS, direcionando as Ordens Judiciais às Instituições que possuem no cadastro CPF ou CNPJ do cliente que está sendo executado. Apontar dentro dessa resolução a vinculação direta das SPSAVs ao sistema CCS, facilita – e muito – o alcance da penhora de criptoativos.

Assim, merece destaque a seguinte menção do Manual de utilização do sistema CCS – Cadastro de Clientes do Sistema Financeiro, disponibilizado pelo Banco Central em julho de 2025:

Todos os clientes das instituições participantes do CCS são alcançáveis pelo Sisbajud - Sistema de Busca de Ativos do Poder Judiciário, sistema sob a gestão do CNJ - Conselho Nacional de Justiça, onde são tratadas ordens judiciais de bloqueio, desbloqueio de contas e transferências de valores para contas judiciais²²⁹. (grifo nosso)

O Manual do BACEN não menciona na parte das Instituições participantes do CCS as SPSAVs, uma vez que é anterior as novas Resoluções do Bacen, que por sua vez, estipula que é preciso comunicar ao CCS, indicando assim que – possivelmente – essas também serão abarcadas pelo sistema.

Por fim, a Resolução 521 estipula regras em relação a algumas atividades das PSAVs (o que inclui as (SPSAVs), que possam ser consideradas como operação de câmbio e capitais internacionais²³⁰.

229 **BANCO CENTRAL DO BRASIL**. Manual de utilização do sistema CCS – Cadastro de Clientes do Sistema Financeiro. Disponível em: https://www.bcb.gov.br/content/acessoinformacao/ccs_docs/manual_do_CCS.pdf Acesso em 22.nov.2025

230 **BANCO CENTRAL DO BRASIL**. Banco Central regulamenta o uso de ativos virtuais e o funcionamento e a autorização das instituições que atuam nesse mercado. Nota de imprensa, 10 nov. 2025. Disponível em: <https://bcb.gov.br/detalhenoticia/20918/nota>. Acesso em: 22 nov. 2025

14. CAMINHOS PARA O DESENVOLVIMENTO DO CRIPTOJUD

Como já abordado anteriormente, o conceito de criptoativo ainda não é muito claro dentro do ordenamento jurídico brasileiro. A Resolução BCB 520, menciona que os ativos sujeitos ao regime da mencionada Resolução são os que estão tratados no Art. 3º, *caput*, da Lei nº 14.478, de 21 de dezembro de 2022, ressalvadas as exceções contidas nos incisos I a IV desse artigo. Nesse sentido:

Art. 3º Para os efeitos desta Lei, considera-se **ativo virtual a representação digital de valor que pode ser negociada ou transferida por meios eletrônicos e utilizada para realização de pagamentos ou com propósito de investimento**, não incluídos:

I - moeda nacional e moedas estrangeiras;

II - moeda eletrônica, nos termos da Lei nº 12.865, de 9 de outubro de 2013;

III - instrumentos que provejam ao seu titular acesso a produtos ou serviços especificados ou a benefício proveniente desses produtos ou serviços, a exemplo de pontos e recompensas de programas de fidelidade; e

IV - representações de ativos cuja emissão, escrituração, negociação ou liquidação esteja prevista em lei ou regulamento, a exemplo de valores mobiliários e de ativos financeiros.

Parágrafo único. Competirá a órgão ou entidade da Administração Pública federal definido em ato do Poder Executivo estabelecer quais serão os ativos financeiros regulados, para fins desta Lei. (grifo nosso).

É, portanto, a representação digital de valor que pode ser negociada ou transferida por meios eletrônicos, bem como utilizada para realização de pagamentos ou com propósito de investimento. Nesse sentido, cabe aludir que o conceito de “representação digital de valor” com “propósito de investimento”, pode acabar esbarrando em alguns conceitos, como por exemplo, o conceito de “*equity token*” que é um tipo de token referenciado a um ativo, sendo, nesse caso,

a representação digital de uma fração de uma propriedade de uma empresa, funcionando – assim – de forma parecida com uma ação tradicional.

equity token ❶ ativos tradicionais de ações, que representam uma participação em determinadas empresas subjacentes, registrados em uma rede baseada em blockchain.²³¹

Não somente isso, mas alguns *tokens* não só representam ativos, como também dão direitos de remuneração por algum empreendimento, inclusive, dando direito ao voto, sendo semelhante a uma estrutura de securitização, de forma que o Parecer de Orientação 40 da CVM configura que – nesses casos – os tokens podem estar debaixo do escopo regulatório da CVM.

As chamadas tokenizadoras e plataformas de *Crowdfunding de investimentos* – até o momento - não estão debaixo do escopo regulatório do BACEN. Sendo assim, um ponto que cabe análise é: esses tokens podem ser considerados penhoráveis? Caso a resposta seja positiva, o penhora deve ser registrada em *blockchain*?

Outro ponto de dúvida é referente aos *tokens* de pagamento, em especial, os criptoativos que estão sendo usados pelo executado na atividade de *Staking*. A resolução BCB 520 aponta o que segue:

Art. 2º Para efeitos desta Resolução, considera-se:

XVI - *staking* de ativos virtuais: o processo por meio do qual uma pessoa, natural ou jurídica, **permite que os seus ativos virtuais sejam bloqueados pela prestadora de serviços de ativos virtuais** com o propósito de participar da validação de transações que ocorrem em um sistema baseado na tecnologia de registros distribuídos ou similar que utiliza como **mecanismos de consenso a prova de participação, podendo usufruir do recebimento de recompensa.**

Em resumo, *staking* é quando uma pessoa (física ou jurídica) mantém o ativo virtual “bloqueado”, em uma espécie de garantia. Esse ativo é “emprestado” para a PSAV para que essa possa utilizar o “direito

231 **Glossário ABCRIPTO**. Versão 1.1, 03 jul. 2023. fl.21 Disponível em: https://backend.abcripto.com.br/media/files/documentsDownloadSection/glossario_abcripto_v1.pdf
Acesso em 16.ou.2025

a voto” no mecanismo de *prove of stake*. Em contrapartida, o usuário ganha um valor referente a permissão desse uso. Ora, se o ativo está “emprestado” para a PSAV, havendo uma ordem de bloqueio, esse ativo pode ser bloqueado? A titularidade permanece sendo do executado?

Outro desafio relevante diz respeito ao destino dos criptoativos após o bloqueio. O Criptojud deverá prever se os ativos permanecerão sob custódia da PSAV em carteira judicial controlada por ente público, ou se haverá conversão imediata dos ativos em moeda fiduciária. Atualmente, nos casos abarcados pelo SISBAJUD, após o bloqueio o ativo permanece na IF, só podendo ser liquidado após pedido de transferência judicial. A transferência judicial só se faz mediante pecúnia, não sendo transferida ação, cota de fundo de investimento ou renda fixa.

Outra dúvida cabível é se será realmente necessária a criação de mais um sistema, ou se bastaria a atualização do sistema SISBAJUD para incluir nos seus envios as SPSAVs e no seu sistema uma resposta de que o ativo bloqueado é um criptoativo. Nesse sentido, caberia sinalizar a cotação do dia e o percentual – caso seja um criptoativo que costuma ser negociado em frações – que foi atingido, de maneira semelhante a uma cota de fundo de investimento. Assim, haveria a comprovação por parte da SPSAV que o que foi bloqueado permaneceu intacto.

Por fim, outra questão que merece enfrentamento é em relação a quantidade que será bloqueada, visto que para que um criptoativo seja liquidado, há algumas taxas a serem pagas, à exemplo do *gas fees*, que são direcionadas aos mineradores (ou validadores) em razão do trabalho computacional exercido para manter a rede segura. Diferentemente do mercado tradicional que os valores de taxas podem ser suportados pelas IFs, no caso das SPSAVs, isso pode ser um problema, porque esse valor não é necessariamente dela, mas sim do minerador que faz funcionar a rede. Nesse sentido, o bloqueio precisaria ser sempre a maior, para considerar esses custos operacionais? Quem suportaria isso?

Todas essas dúvidas precisam ser enfrentadas para que seja possível criar um sistema seguro e funcional. Para solucionar isso é possível seguir em duas frentes: a primeira é o diálogo com instituições já consolidadas e que possuem a expertise de sistemas como SISBAJUD. Ao olhar para o mercado tradicional, o ecossistema cripto pode encontrar os caminhos nos quais se assemelha e criar soluções naquilo que se diferencia. A segunda frente é na criação de uma regulação pelo CNJ semelhante à regulação SISBAJUD, apontando cada uma dessas questões e direcionando o mercado no melhor sentido possível. Assim, a penhora de ativos virtuais poderá funcionar de uma maneira clara, efetiva e segura, fortalecendo, assim, o Sistema Financeiro Nacional como um todo.

CONSIDERAÇÕES FINAIS

A análise desenvolvida ao longo deste trabalho evidencia que o avanço dos criptoativos no Brasil impõe desafios significativos ao ordenamento jurídico, especialmente no âmbito da execução civil. A natureza descentralizada desses ativos, aliada à multiplicidade de plataformas e modelos de custódia, ainda representa um obstáculo concreto para a efetividade das decisões judiciais envolvendo penhora.

Apesar desse cenário desafiador, observa-se um movimento consistente de evolução normativa e institucional. A Lei 14.478/2022 inaugurou o Marco Legal dos Criptoativos, estabelecendo diretrizes gerais para o setor. Em complemento, as Consultas Públicas do Banco Central e, posteriormente, as Resoluções BCB nº 519, 520 e 521, consolidaram um arcabouço regulatório mais robusto para as prestadoras de serviços de ativos virtuais, trazendo maior segurança jurídica ao mercado e criando condições mais favoráveis para o cumprimento de ordens judiciais.

A proposta do sistema Criptojud emerge nesse contexto como uma solução necessária e alinhada ao processo de modernização da Justiça brasileira. Embora sua implementação envolva desafios técnicos, jurídicos e operacionais, o sistema representa um passo

essencial para superar a dependência de procedimentos manuais, lentos e frequentemente ineficazes.

As recentes resoluções do Banco Central reforçam essa perspectiva ao exigir que as SPSAVs e PSAVs estejam sediadas no território nacional, submetidas à supervisão regulatória e comunicando informações ao CCS. Esse novo cenário normativo contribui para ampliar a viabilidade do Criptojud, aproximando o ecossistema cripto do modelo já consolidado no SISBAJUD.

Em conclusão, ainda que persistam desafios regulatórios, técnicos e interpretativos, o Brasil avança de forma significativa rumo à construção de um ambiente jurídico capaz de lidar com a crescente presença dos criptoativos no patrimônio dos indivíduos e empresas. A efetividade da penhora desses ativos dependerá, em grande medida, da integração entre a regulação financeira, o desenvolvimento tecnológico e a adaptação das práticas judiciais. O diálogo contínuo entre o Direito e a tecnologia, aliado ao fortalecimento das instituições reguladoras, será determinante para assegurar a proteção dos credores, a segurança jurídica dos agentes econômicos e o desenvolvimento sustentável desse novo mercado.

REFERÊNCIAS

ABCRIPTO. Glossário ABCRIPTO. Versão 1.1, 03 jul. 2023. fls. 3, 7, 15, 17–18, 21, 40. Disponível em: https://backend.abcripto.com.br/media/files/documentsDownloadSection/glossario_abcripto_v1.pdf. Acesso em: 16 out. 2025.

AMID. Diretiva (UE) 2018/843 (AMLD5). Disponível em: <https://eur-lex.europa.eu/eli/dir/2018/843/oj/eng>. Acesso em: 16 out. 2025.

ARANHA, Cristian. Bitcoin, blockchain e muito dinheiro. 4. ed. Rio de Janeiro: Valentina, 2022. fls. 31–32, 35, 49, 77.

BANCO CENTRAL DO BRASIL. Banco Central regulamenta o uso de ativos virtuais e o funcionamento e a autorização das instituições que atuam nesse mercado. Nota de imprensa, 10 nov. 2025. Disponível em: <https://bcb.gov.br/detalhenoticia/20918/nota>. Acesso em: 22 nov. 2025.

BANCO CENTRAL DO BRASIL. Das corretoras de ativos virtuais. Art. 10. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolução%20BCB&numero=520> . Acesso em: 22 nov. 2025.

BANCO CENTRAL DO BRASIL. Manual de utilização do sistema CCS – Cadastro de Clientes do Sistema Financeiro. Disponível em: https://www.bcb.gov.br/content/acessoinformacao/ccs_docs/manual_do_CCS.pdf. Acesso em: 22 nov. 2025.

BANCO CENTRAL DO BRASIL. Resolução BCB nº 520, de 10 nov. 2025. Arts. 1º, 14. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolução%20BCB&numero=520>. Acesso em: 22 nov. 2025.

BINANCE HOLDING UY S.A. Resposta à consulta pública do Banco Central do Brasil. fl. 24. Disponível em: <https://www3.bcb.gov.br/>

audpub/DetalharAudilanciaPage?6&audienciaId=702. Acesso em: 12 out. 2025.

BRASIL. Decreto nº 11.563, de 13 de junho de 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11563.htm. Acesso em: 15 out. 2025.

BRASIL. Lei nº 6.385, de 7 dez. 1976, e Lei nº 10.303, de 31 out. 2001. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l6385.htm
https://www.planalto.gov.br/ccivil_03/leis/LEIS_2001/L10303.htm
Acesso em: 16 out. 2025.

BRASIL. Lei nº 12.865, de 9 out. 2013. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12865.htm. Acesso em: 15 out. 2025.

BRASIL. Lei nº 14.478, de 21 dez. 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/lei/l14478.htm. Acesso em: 16 out. 2025.

BRASIL. Receita Federal do Brasil. Instrução Normativa RFB nº 1.888, de 3 maio 2019. Art. 5º, inc. II e parágrafo único. Disponível em: <https://normasinternet2.receita.fazenda.gov.br/#/consulta/externa/100592/visao/multivigente>. Acesso em: 16 out. 2025.

CAMBRIDGE DICTIONARY. LatAm. Disponível em: <https://dictionary.cambridge.org/pt/dicionario/ingles/latam>. Acesso em: 12 out. 2025.

CÂMARA, Alexandre F. O Novo Processo Civil Brasileiro. 8. ed. Rio de Janeiro: Atlas, 2022. E-book. p. 397.

CHAINALYSIS. Latin America is one of the world's most dynamic crypto markets. Disponível em: <https://www.chainalysis.com/blog/latin-america-crypto-adoption-2025/>. Acesso em: 12 out. 2025.

CNN BRASIL. Entenda a diferença entre criptomoeda e moeda digital. Disponível em: <https://www.cnnbrasil.com.br/economia/financas/entenda-a-diferenca-entre-criptomoeda-e-moeda-digital-como-a-estudada-pelo-bc/>. Acesso em: 15 out. 2025.

CNJ. CriptoJud: novo sistema possibilita consulta on-line da posse de criptoativos por devedores. Disponível em: <https://www.cnj.jus.br/criptojud-novo-sistema-possibilita-consulta-on-line-da-posse-de-criptoativos-por-devedores/>. Acesso em: 16 out. 2025.

CNJ. Portaria SEP nº 2/2025. Disponível em: <https://atos.cnj.jus.br/files/original200313202508066893b50119290.pdf>. Acesso em: 16 out. 2025.

COINTELEGRAPH. El Salvador comemora aniversário do Bitcoin. Disponível em: <https://br.cointelegraph.com/news/el-salvador-bitcoin-anniversary-mixed-results-4-years>. Acesso em: 16 out. 2025.

CRUSTLAB. Comparison of DAG vs Blockchain: Differences, Pros, and Cons. 23 jul. 2025. Disponível em: <https://crustlab.com/blog/dag-vs-blockchain/>. Acesso em: 16 out. 2025.

CUNHA, Gustavo. A tokenização do dinheiro. São Paulo: Almedina Brasil, 2024. p. 38, 40, 46.

CVM. Edital de Consulta Pública SDM nº 05/25. Disponível em: https://conteudo.cvm.gov.br/audiencias_publicas/ap_sdm/2025/sdm0525.html. Acesso em: 16 out. 2025.

CVM. Ofício-Circular nº 4/2023/CVM/SSE. Disponível em: <https://conteudo.cvm.gov.br/legislacao/oficios-circulares/sse1/oc-sse-0423.html>. Acesso em: 16 out. 2025.

CVM. Ofício-Circular nº 6/2023/CVM/SSE. Disponível em: <https://conteudo.cvm.gov.br/export/sites/cvm/legislacao/oficios-circulares/sse1/anexos/oc-sse-0623.pdf>. Acesso em: 16 out. 2025.

CVM. Parecer de Orientação nº 40, de 11 out. 2022. fls. 4–6. Disponível em: <https://conteudo.cvm.gov.br/legislacao/pareceres-orientacao/pare040.html>. Acesso em: 16 out. 2025.

CVM. Resolução CVM nº 88, de 2022. Disponível em: <https://conteudo.cvm.gov.br/legislacao/resolucoes/resol088.html>. Acesso em: 16 out. 2025.

ECB – EUROPEAN CENTRAL BANK. Virtual currency schemes. Oct. 2012. Disponível em: <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>. Acesso em: 15 out. 2025.

FCA – FINANCIAL CONDUCT AUTHORITY. Guidance on Cryptoassets: Policy Statement PS19/22. July 2019. Disponível em: <https://www.fca.org.uk/publication/policy/ps19-22.pdf>. Acesso em: 22 nov. 2025.

FILHO, Sergio Zahr. Penhora: exame da técnica processual à luz da realidade econômica social. São Paulo: USP, 2009. fls. 123–124. Disponível em: https://teses.usp.br/teses/disponiveis/2/2137/tde-15062011-162250/publico/DISSERTACAOFINAL_CD_.pdf. Acesso em: 21 set. 2025.

MOREIRA, José Carlos Barbosa. O Novo Processo Civil Brasileiro. 29. ed. Rio de Janeiro: Forense, 2012. p. 237.

OECD. Understanding the tokenisation of assets in financial markets. Paris: OECD, 2021. Disponível em: https://www.oecd.org/content/dam/oecd/en/publications/reports/2021/11/understanding-the-tokenisation-of-assets-in-financial-markets_2e657111/c033401a-en.pdf. Acesso em: 22 nov. 2025.

PORTAL DO BITCOIN. CriptoJud: novo sistema da Justiça vai facilitar bloqueio de criptomoedas em exchanges. Disponível em: <https://portaldobitcoin.uol.com.br/criptojud-novo-sistema-da-justica-vai-facilitar-bloqueio-de-criptomoedas-em-exchanges/>. Acesso em: 16 out. 2025.

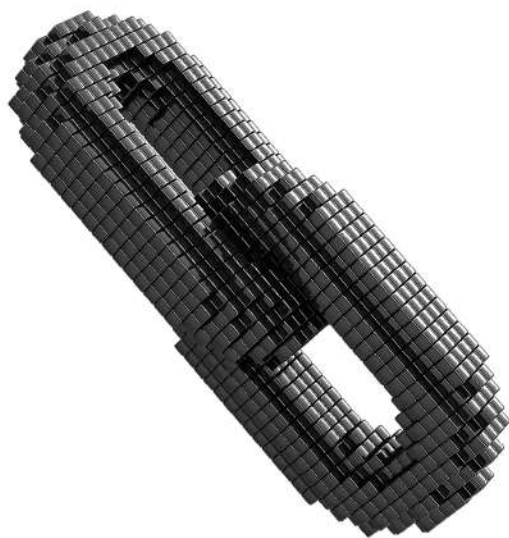
OAM ADVOGADOS. Criptojud deve agilizar penhora de criptoativos. Disponível em: <https://www.oam.adv.br/2024/11/criptojud-deve-agilizar-penhora-de-criptoativos-mas-nao-evita-fraudes/> Acesso em: 16 out. 2025.

STJ - SUPERIOR TRIBUNAL DE JUSTIÇA. REsp 2127038 - SP. Brasília, 18 fev. 2025. Disponível em: <https://processo.stj.jus.br/processo/pesquisa/?aplicacao=processos.ea&tipoPesquisa=tipoPesquisaGenerica&termo=REsp%202127038>. Acesso em: 16 out. 2025.

XP INVESTIMENTOS. O que é uma criptomoeda? Disponível em: <https://atendimento.xpi.com.br/artigo/2169-o-que-e-uma-criptomoeda>. Acesso em: 15 out. 2025.

PARTE III

TRANSFORMAÇÃO DIGITAL DO ESTADO
E INOVAÇÃO PÚBLICA



8. CONTRIBUTOS DA DIGITIZAÇÃO DO REGISTRO DE IMÓVEIS PARA EFETIVAÇÃO DA AGENDA BRASILEIRA PARA CIDADES INTELIGENTES: GOVERNANÇA DE DADOS E POLÍTICAS GEORREFERENCIADAS

Luís Henrique de Menezes Acioly

Especialista em Direito Digital pelo Instituto de Tecnologia e Sociedade do Rio de Janeiro – ITS Rio em parceria com o Centro de Estudos e Pesquisas no Ensino do Direito da Universidade do Estado do Rio de Janeiro (CEPED/UERJ). Graduado em Direito pelo Centro Universitário Ruy Barbosa - UniRuy. Coordenador de Pesquisa do Grupo de Estudos em Tecnologia, Informação e Sociedade - GETIS/CNPq. Advogado.Técnico em Química pelo Instituto Federal da Bahia (IFBA).

INTRODUÇÃO

A Carta Brasileira para Cidades Inteligentes, documento político democrático que expressa uma agenda pública para a transformação digital dos centros urbanos (“Agenda Brasileira para Cidades Inteligentes”), propõe o estabelecimento de sistema de gestão de dados e adoção de modelos inovadores de governança urbana.

A tecnologia constitui o eixo de transformação digital da urbe, no escopo de viabilizar soluções inovadores para questões ambientais, econômicas e socioculturais. O tema de cidade inteligente se insere em uma perspectiva de criar oportunidades, reduzir desigualdades e oferecer serviços com excelência, tendo a centralidade humana como objetivo, consistente em melhorar a vida da população. A cidade não é o palco, mas se posiciona como atriz, envolvendo-se em projetos de negociação, planejamento e gestão territorial, com catalisadora da inovação científica (Duarte, 2005).

A implementação de projetos dessa envergadura em âmbito nacional enfrenta obstáculos significativos, por “falta de

regulamentação específica e à necessidade de um planejamento urbano integrado e sustentável” (Faleiros Júnior, 2024, p. 114).

Nesse contexto, a gestão do solo urbano, dos espaços públicos e da função social da propriedade perpassa pelo registro público de imóveis, que congrega informações sobre as relações de direito imobiliário, inclusive correlacionadas a áreas públicas e privadas.

Com o atual panorama de prestação dos serviços de registro de imóveis por meio da *Internet*, a gestão de dados relativos à demografia imobiliária e ao direito à propriedade e à moradia regularizada é potencializada. Esse panorama fomenta uma interação latente com o Poder Público municipal e contribuindo para o alcance dos objetivos da Carta, cujo sentido e alcance é objeto da presente pesquisa.

Tem-se como problema de pesquisa investigar de que maneira, e a partir de quais fundamentos, o processo de digitização do registro de imóveis pode contribuir para a efetivação da Agenda Brasileira para Cidades Inteligentes.

O presente constructo pretende, assim, analisar o eixo técnico-jurídico performado pela governança de dados e pela gestão de políticas públicas baseadas em dados nos objetivos estratégicos da Carta Brasileira para Cidades Inteligentes. Assim como busca examinar o panorama jurídico atual da inserção do registro de imóveis no ambiente digital, com ênfase no Sistema do Registro Eletrônico de Imóveis e na governança de dados de titularidade imobiliária e georreferenciamento de bens imóveis.

Preconizando-se a interdisciplinaridade da ciência jurídica interseccionada a outras áreas das ciências sociais, o presente estudo apresenta uma abordagem científica de método hipotético-dedutivo, na medida em que parte de premissas, valida-as em suas conjecturas e as examina para alcançar uma corroboração (Henriques; Medeiros, 2017). Quanto ao método de pesquisa, o presente estudo a pesquisa bibliográfica, ou de fontes secundárias (Marconi; Lakatos, 2021), isto é, o desenvolvimento com base em material já elaborado concernente a fontes bibliográficas documental e doutrinária (Gil, 2002).

A fonte documental concerne a legislação brasileira e documento de caráter político, a Carta Brasileira para Cidades Inteligentes. A fonte doutrinária, por sua vez, se dará através de coleta de dados em livros, dissertações e artigos, repositados em bases de dados eletrônicas – *Scientific Electronic Library Online* (SciELO) e *Google Acadêmico* –, tendo como descritores: Cidades Inteligentes; *Smart Cities*; Governança Digital; Governança de Dados; Dados Imobiliários; Dados Pessoais; Proteção de Dados; Registro de Imóveis; SREI; Digitização; Interoperabilidade; Política Pública baseada em dados; Direito à Moradia; Urbanismo.

1. ANÁLISE DE EIXOS NA CARTA BRASILEIRA PARA CIDADES INTELIGENTES

O avanço da urbanização tem produzido efeitos positivos à vida em sociedade, como a criação de novas oportunidade de emprego, a melhoria do padrão de consumo e poder aquisitivo e a promoção da integração social (Belli; Doneda, 2021). No entanto, esse processo também projeta efeitos indesejados, que demandam soluções eficientes, rápidas e eficazes, para as quais as tecnologias de informação e comunicação constitui base.

O conjunto heterogêneo de iniciativas e projetos²³² que visam a transformação do espaço urbano por meio da tecnologia, tendo em vista viabilizar o planejamento territorial, o engajamento, a participação cidadã e as políticas de mobilidade²³³, tem sido denominado de “*Smart Cities*”, ou “Cidades Inteligentes” (Antonialli; Kira, 2020; Maia; Figueira, 2024).

232 Deve-se ressaltar que, ainda que exista uma convergência temática em relação a possíveis conceitos, não há um consenso (Maia; Figueira, 2024). Lima (2024) aponta que foram catalogadas, em 2024, mais de 100 conceituações distintas, publicadas por organizações públicas e privadas, em suas próprias atribuições.

233 Embora comumente associado às tecnologias de informação e comunicação, a base conceitual das cidades inteligentes não se associa expressamente à técnica utilizada, focando em elementos finalísticos, como a infraestrutura física e de rede, o fornecimento eficiente de serviços públicos e o desenvolvimento social, ambiental e econômico (Kominos, 2009; Belli; Doneda, 2021).

Os gestores municipais têm, em razão da tecnologia, um volume maior de dados à sua disposição, em virtude da multiplicação de dispositivos conectados à *Internet*, dos menores custos de armazenamento de informações em nuvem e do aperfeiçoamento das técnicas de *big data analysis* (Antonialli; Kira, 2020), o que demanda estratégia na aplicação desse arcabouço.

O Ministério do Desenvolvimento Regional do Brasil, no âmbito do projeto de cooperação “Apoio à Agenda Nacional de Desenvolvimento Urbano Sustentável no Brasil -ANDUS” junto a *Deutsche Gesellschaft für Internationale Zusammenarbeit* (GIZ) GmbH, a agência de cooperação alemã (Sousa Júnior, 2021), desenvolveu a “Carta Brasileira para Cidades Inteligentes” ou “Carta”²³⁴.

Ainda que se trate de um documento emitido pelo Poder Público Federal, não consiste em regulamentação, mas constitui materialização de uma política de fomento ao desenvolvimento de cidades inteligentes, de forma segura e eficiente. A Carta pretende: (i) a construção de um posicionamento nacional sobre o tema, a partir de uma definição conceitual; (ii) a formulação de uma agenda pública por municípios e outras instituições; (iii) a articulação e integração de iniciativas; e (iv) a orientação da ação pública a nível local (Bruno *et al.*, 2021).

O documento se estrutura em 8 objetivos estratégicos e 163 recomendações direcionadas a segmentos de público-chave (Sousa Júnior, 2021), dentre os quais encontram-se a integração da transformação digital nas políticas, programas e ações de desenvolvimento urbano sustentável, e o estabelecimento de sistemas de governança de dados.

234 O formato de “carta” foi escolhido como suporte por estar alinhado à finalidade do documento. Ao longo da história, esse gênero textual tem servido como um instrumento de referência para a ação política, permitindo que grupos de atores, setores, comunidades ou instituições expressem publicamente seus pontos de vista e orientem caminhos de atuação diante de questões de relevância social. Nesse sentido, a “carta” também cumpre a função de explicitar compromissos assumidos coletivamente em torno de um projeto comum, cuja dimensão sistêmica ultrapassa a capacidade de realização de uma única instituição de forma isolada (Bruno *et al.*, 2021, p. 178).

1.1. A Governança de Dados como Objetivo Estratégico da Carta

É latente à condução de projetos de urbanização inteligente a utilização massiva de dados pessoais, seja por meio da captura de informações espaciais por sensores²³⁵ e câmeras (Nazareno, 2021), ou na identificação de uso de aplicativos e aparelhos conectados a determinadas redes (Faleiros Júnior, 2024). A pandemia de Covid-19 demonstrou como estruturas algorítmicas podem ser utilizadas para a gestão do espaço urbano afim de evitar aglomerações e estancar a disseminação de agente patológico, evidenciando o potencial benéfico do uso de dados pessoais em aplicação de *Internet das Coisas* (Faleiros Júnior, 2024).

Para tratamento dessas informações, gestores de projetos de cidades inteligentes valem-se de estruturas de *big data* (Mayer-Schönberger; Cukier, 2013), em que os dados coletados massivamente²³⁶ não são filtrados ou estruturados de acordo com a respectiva finalidade, e que acabam armazenados em serviços de nuvem, exposto a vulnerabilidades de cibersegurança (Nazareno, 2021; Lima, 2024).

A utilização de dados não estruturados pode gerar riscos operacionais e jurídicos, resultantes do volume excessivo de informações e da inobservância de diretrizes da Lei Geral de Proteção

235 Acerca do tratamento de dados pessoais por coleta via sensores, didática é a explicação dada pela Agência Nacional de Proteção de Dados (2024, 9): “A dinâmica funciona basicamente da seguinte forma: sensores (incluindo câmeras) distribuídos pela cidade captam dados dos mais diversos (inclusive dados pessoais), que são transmitidos por meio de uma rede de comunicação de dados até um local em que serão processados (esforço computacional), gerando informação estruturada para a tomada de decisão”.

236 Como apontado, por Lim, Kim e Maglio (2018) os dados de cidades inteligentes podem ser advindos de compartilhamento por empresas, por determinação administrativa ou em razão de benefícios fiscais, ou coletados diretamente pelo Poder Público, e seus fornecedores, junto aos cidadãos e visitantes. No âmbito do compartilhamento por empresas, Antonialli e Kira (2020) relacionam o caso da Uber, que em razão da Resolução n. 19 da Secretaria Municipal de Mobilidade e Transporte (SMT/CMUV), possui o dever de disponibilização à prefeitura municipal de São Paulo, dados sobre a prestação do serviço. Na forma da Resolução n. 21 do mesmo órgão, os dados devem ser agrupados em: (i) sobre as corridas; inclusive com organização visual georreferenciada (mapa); e (ii) sobre os condutores.

de Dados Pessoais (Lei Federal n. 13.709, de 2018), especialmente quanto ao princípio da necessidade (Lima, 2024). Nessa linha, também há o risco de converter a tecnologia em aparato de um Estado policaiesco, mediante constituição de vigilância constante (Faleiros Júnior, 2024). A relação com *stakeholders* pode, ademais, desencadear o uso comercial de dados tratados em razão do engajamento de fornecedores nas tecnologias usadas nesses projetos (ANPD, 2024).

Em caráter mais pragmático, Lim, Kim e Maglio (2018) e Nazareno (2021) atribuem como principais desafios inerentes ao uso de *big data* em iniciativa de *smart cities*: (i) o gerenciamento da qualidade dos dados, (ii) a integração das informações, (iii) a privacidade dos usuários, (iv) o entendimento das necessidades de todos os envolvidos, (v) o melhoramento das informações geográficas, e (vi) o desenho de serviços inteligentes.

Seguindo essa linha, a Carta Brasileira para Cidades Inteligentes consigna como seu Objetivo Estratégico n. 3: “Estabelecer sistemas de governança de dados e de tecnologias, com transparência, segurança e privacidade”, performado por recomendações como (Sousa Júnior, 2021, p. 26):

3.1. Segurança cibernética: Garantir a segurança cibernética em infraestrutura, dispositivos, sistemas, dados e informações digitais. Estabelecer diretrizes, normas e procedimentos que avaliem, melhorem e validem a confiabilidade de hardwares, sistemas operacionais, dispositivos de acesso pessoal e ferramentas individuais;

3.2. Proteção geral de dados pessoais: Garantir a proteção de dados pessoais, aderindo completamente à Lei Geral de Proteção de Dados Pessoais (LGPD). Respeitar a titularidade da pessoa natural sobre os seus próprios dados pessoais, garantindo, ao mesmo tempo, os direitos fundamentais de liberdade, intimidade e privacidade. Assegurar que o compartilhamento de dados pessoais obedeça aos princípios de finalidade e transparência. Para possibilitar essas ações, estabelecer normas e procedimentos que viabilizem o desenvolvimento seguro e ético de negócios inovadores baseados em dados.

3.2.1. Normas locais de proteção de dados pessoais: Apoiar os municípios para que adéquem normas e procedimentos à Lei Geral de Proteção de Dados Pessoais (LGPD). Regular de forma prioritária o tratamento de dados em serviços públicos essenciais e os cadastros em serviços digitais.

3.4. Interoperabilidade: Garantir a interoperabilidade ao implementar soluções de tecnologias de informação e comunicação em governos, em iniciativas interinstitucionais, inclusive público-privadas.

A constitucionalização formal da proteção de dados pessoais, por meio da Emenda Constitucional n. 115, de 2022, reforça o sistema de *enforcement* da LGPD e reconhece a “autodeterminação informativa como consectária do livre desenvolvimento da personalidade” (Acioly *et al.*, 2024, p. 8). Desse reconhecimento, devem ser adotados, por todos os agentes envolvidos medidas de observância à LGPD, bem como de fiscalização e governança nodal para consolidação de um sistema robusto de respeito a direitos fundamentais²³⁷ (Bioni, 2022).

Belli e Doneda (2021) apontam os seguintes parâmetros básicos para conformidade de cidades inteligentes à LGPD: (i) observância aos princípios da finalidade e da necessidade, em conjunto com a aplicação de técnicas de anonimização; (ii) direito à revisão de decisão tomada por sistemas automatizados; (iii) adoção de medidas técnicas e administrativas para segurança e prevenção contra incidentes, de acordo com o estado da arte; (iv) realização de relatórios de impacto à proteção de dados pessoais.

A Carta Brasileira para Cidades Inteligentes caminha nessa linha, ao recomendar expressamente o cumprimento pelos municípios das obrigações inerentes à proteção de dados pessoais, inclusive por meio de mecanismos de cibersegurança e interoperabilidade de

237 Como exemplo de aplicação dessa perspectiva, Antonialli e Kira (2020) apontam o caso do Reino Unido que, ao desenvolver medidores inteligentes do consumo de energia elétrica, que podem capturar informações sobre a rotina dos cidadãos britânicos, incorporou princípios de *privacy by design*, para minimizar os riscos inerente ao tratamento de dados pessoais.

comunicação a nível de dados com órgãos governamentais e iniciativas interinstitucionais.

1.2. O Georreferenciamento de Dados nos Objetivos Estratégicos da Carta

A adoção de políticas públicas baseadas em evidências também se apoia em informações geoespaciais do solo urbano, dos serviços executados e de áreas prioritárias para atendimento a necessidades básicas da população.

Lim, Kim e Maglio (2018) atribuem à ausência de um sistema de informações geográficas (SIG) a impossibilidade de análise da dados por região da cidade, em questões como a avaliação da eficiência de rotas de ônibus e a identificação de necessidades regionais em projetos de saúde. Em projetos de cidades inteligentes, a gestão geográfica das informações deve ser robustecida, para viabilizar a execução dos objetivos de política pública e melhorar a aceitação por cidadãos, visitantes e funcionários (Lim; Kim; Maglio, 2018).

Seguindo essa linha, a Carta Brasileira para Cidades Inteligentes prevê em suas recomendações o georreferenciamento de dados²³⁸, em uma perspectiva de gestão territorial adequada, relevante e integrada (Sousa Júnior, 2021, p. 27-28):

3.5.1. Registros administrativos: Coletar, sistematizar, digitalizar, georreferenciar e disponibilizar dados e informações gerados ao executar políticas públicas e ao prestar serviços públicos, em todos os níveis de governo. Tratar e anonimizar dados sensíveis para possibilitar sua abertura. Todas as etapas devem cumprir as políticas de dados abertos e os padrões de interoperabilidade existentes para o nível de governo que executa as ações.

238 Conforme Mallmann *et al.* (2024, pp. 234-235): “O georreferenciamento (ou geo) é o procedimento técnico pelo qual se realiza o levantamento geodésico e topográfico¹⁰ de determinado imóvel ou parcela deste, permitindo que sua caracterização (limites, confrontações, características, perímetro e área) e sua localização (local específico no globo terrestre, mediante coordenadas geodésicas em pontos de referência) sejam identificadas e descritas com precisão posicional absoluta”.

3.5.2. Dados geoespaciais: Fortalecer a Infraestrutura Nacional de Dados Espaciais como plataforma que facilita o intercâmbio de dados geoespaciais. Estabelecer a Política Nacional de Geoinformação e consolidar um vocabulário uniforme e específico em sistemas de informação geográfica urbana.

3.8. Gestão territorial integrada: Usar sistemas de planejamento integrado e de gestão territorial integrada, com base em plataformas interoperáveis (que trabalham em conjunto para a troca eficaz de informações) de dados georreferenciados (plataformas que possibilitem a troca eficaz de dados com localização geográfica), em todos os níveis de governo. Os sistemas devem ser adequados às diferentes escalas das políticas públicas e respeitar a proteção de dados pessoais. Também devem atender às especificidades, demandas e capacidades locais, nos casos de sistemas municipais.

Nessa feita, Justi (2021) propõe modelos de levantamento geoespacial do espaço urbano, para fins de consolidação de dados para projetos de cidades inteligentes, sendo eles: (i) o levantamento de elementos da cidade, como edificações, ruas e construções, baseado em captura de imagens por drones ou imagens de satélite; (ii) levantamento de informações relacionadas a logradouros públicos, como sinalizações e equipamentos instalados pelo Poder Público, para fins de gestão de obras e manutenção; e (iii) levantamento da infraestrutura urbana, como tubulações, fiações enterradas e fornecimento de água e água e esgoto.

Justi (2021) sustenta, ainda, a criação de um ambiente comum de informações entre os envolvidos nessas operações, no escopo de viabilizar um banco de dados sobre legislações, materiais e equipamentos, contratos e informações cadastrais em lote, inclusive de ordem tributária e fiscalizatória. Nesse contexto, a Carta Brasileira para Cidades Inteligentes estabelece em suas recomendações, medidas para integração de cadastros multifinalitários e análise de dados georreferenciados (Sousa Júnior, p. 20):

1.5.1.1. TICs para o diagnóstico e a gestão urbana: Usar ferramentas de geoprocessamento (processamento de dados com

localização geográfica) para entender melhor os fenômenos urbanos e para aperfeiçoar a capacidade de gestão dos governos locais. Incorporar nessas ações mecanismos inovadores da ciência de dados. Exemplos: (1) Inteligência Artificial (AI); e (2) análise de grandes quantidades de dados anonimizados (sem elementos que identifiquem as pessoas), conhecidos como Big Data. Respeitar a Lei Geral de Proteção de Dados Pessoais (LGPD).

1.5.1.5. Cadastros territoriais integrados: Apoiar municípios e órgãos interfederativos (que representam mais de um ente federativo - União, Estados, Distrito Federal e Municípios) a elaborar, revisar e integrar as suas bases territoriais. Essas bases podem ser bases cartográficas, cadastros imobiliários ou Cadastros Técnicos Multifinalitários (de diversas finalidades) – CTM. Além disso, apoiar a integração dessas bases com os sistemas de informações geográficas locais. Essas ações devem se basear em metodologias e recursos adequados às diferentes realidades e às tipologias municipais e supramunicipais (agrupamentos de municípios) da Política Nacional de Desenvolvimento Urbano (PNDU).

A partir do georreferenciamento de informações, a gestão municipal pode viabilizar operações urbanas consorciadas²³⁹, e estabelecer mecanismos eficazes de governança de dados em caráter gráfico e relevante (Kominos, 2009), auxiliando na tomada de decisões²⁴⁰. A Carta Brasileira para Cidades Inteligentes expõe uma relevante preocupação com a precisão das evidências, na estrutura da governança das informações tratadas de forma integralizada para construção de políticas públicas municipais.

239 Conforme Berndsen (2019, p.102) “as Operações Urbanas Consorciadas, referem-se a um conjunto de intervenções e medidas, coordenadas pelo poder público municipal, com a finalidade de preservação, recuperação ou transformação de áreas urbanas contando com a participação dos proprietários, moradores, usuários permanentes e investidores privados”.

240 Aponta-se nesse sentido, a experiência da cidade de São Paulo que, tornou público dados inerentes ao cadastro de imóveis para fins de Imposto Territorial e Predial Urbano (IPTU), dentre os quais o nome da pessoa física e/ou jurídica proprietária, a metragem dos imóveis, o tipo de construção e o tipo de uso, através da plataforma gráfica GeoSampa, que reúne essas informações em um mapa georreferenciado (Antonialli; Kira, 2020).

2. CONTEXTO HISTÓRICO-NORMATIVO DA CONSOLIDAÇÃO DO SISTEMA DO REGISTRO ELETRÔNICO DE IMÓVEIS (SREI)

Em se tratando de dados referentes à propriedade imobiliária, as serventias extrajudiciais possuem um conglomerado de informações úteis aos objetivos das cidades inteligentes. O registro público de imóveis, de titularidade do Estado e sob delegação constitucional ao particular, constitui repositório de dados (Chezzi, 2021) concernentes às informações sobre qualificação objetiva atual dos bens imóveis registrados, e concernentes às modificações dos direitos de propriedade e alterações substanciais à estrutura física dos bens e logradouros públicos, em perspectiva histórica.

Essa característica representa o potencial de contribuição com políticas públicas baseadas em dados georreferenciados, especialmente diante do novo panorama de digitização dos serviços extrajudiciais e consolidação do registro eletrônico de imóveis (Martins, 2022).

Diferente de outras atividades, em que a regulamentação vem a reboque, o registro imobiliário brasileiro, em sua maior parte, teve o seu desenvolvimento decorrente do avanço normativo, em atenção ao constante aperfeiçoamento das técnicas jurídicas e arquivísticas. Foi assim com a Lei Federal n. 6.015, de 1973, que instituiu o sistema de fôlio real, em que se deu preponderância à matrícula com cerne da atividade registral (Ribeiro, 2019).

Esse aprimoramento técnico e jurídico ocorreu como reação ao sistema de transcrições que, conforme assevera Fioranelli (2014), tornava obrigatória a repetição da caracterização do bem registrado a cada vez que sua propriedade era transmitida ou de qualquer outra forma era onerado. Com o sistema de matrículas, os imóveis passaram a ter um registro concentrado, fazendo-se constar toda a cadeia dominial do bem (Castro, 2021), assim como sua realidade, observando-se a devida qualificação objetiva e modificações estruturais (Ribeiro, 2019).

A eficiência desse sistema deu embasamento à ampliação do registro de imóveis, dando ao oficial registrador o protagonismo na

proteção do direito de propriedade a partir da qualidade da informação vinculado à matrícula imobiliária (Ribeiro, 2019). No entanto, na contemporânea sociedade da *hyper-informação* (Madalena, 2019), a *Internet* tem assumido o lugar de protagonista das relações sociais, promovendo mudanças em termos culturais, econômicos, jurídicos e governamentais (Castells, 2002).

Sem embargo de ressaltar a profundidade do tema “Governo como Plataforma”²⁴¹, a remodelagem da prestação de serviços públicos por meio da *Internet* também alcançou o registro imobiliário, notadamente a partir da Lei Federal n. 11.977, de 2009. Esse diploma deu luz à possibilidade de recepção e emissão de documentos eletrônicos, desde que observados os requisitos da Infraestrutura de Chaves Públicas Brasileira – ICP Brasil e a arquitetura e-PING.

A Lei Federal n. 11.977, de 2009, também se arvorou a estabelecer o dever de os serviços de registros públicos instituírem um “sistema do registro eletrônico”, conforme regulamentação própria. O Conselho Nacional de Justiça, seguindo essa diretriz, editou a sua Recomendação n. 14, de 2014, para orientar as Corregedorias Gerais de Justiça, das respectivas Unidades da Federação, na implementação de um “sistema do registro eletrônico de imóveis” (Gruber, 2016; Castro, 2021).

A Recomendação n. 14, de 2014, estabeleceu que fossem observados os parâmetros definidos pela Associação do Laboratório de Sistemas Integráveis Tecnológicos, na implementação desse sistema, sem trazer maiores definições (Assad, 2016; Tavares, 2018).

No entanto, a Corregedoria Geral de Justiça de São Paulo (CGJ-SP) já havia editado, em 2012, o seu Provimento n. 42, fornecendo diretrizes para a implantação do Sistema do Registro Eletrônico de Imóveis (SREI) naquele Estado, dando forma à Central de Serviços Eletrônicos Compartilhados dos Registradores de Imóveis como ponto

241 Conforme Faleiros Júnior (2022, p. 6) elucida, a teoria do “Governo como Plataforma” se fundamenta em estudo desenvolvido por O’Reilly (2011) e refere-se ao “dever estatal de fomento à implementação de infraestrutura tecnológica voltada a facilitar a interação entre diversos agentes, com finalidades variadas”.

de acesso a serviços do registro imobiliário através da *Internet*²⁴² (Assad, 2016; Castro, 2021). À luz dessa norma, o desenvolvimento, a operação e administração do SREI no estado paulista seria de responsabilidade da ARISP – Associação de Registradores Imobiliários de São Paulo²⁴³ (Assad, 2016; Castro, 2021).

Em 2015, o Conselho Nacional de Justiça editou o Provimento n. 47, traçando as diretrizes técnicas e jurídicas que deveriam ser observadas na implementação do Sistema do Registro Eletrônico de Imóveis (SREI) no âmbito de cada Estado e do Distrito Federal (Gruber, 2016). A partir dessa norma, promoveu-se a criação das centrais de serviço eletrônico compartilhados, administradas de forma local, mediante ato normativo promovido por cada Corregedoria Geral de Justiça²⁴⁴.

O Provimento n. 47, de 2015, do CNJ, trouxe a necessidade de homogeneidade das centrais eletrônicas em cada um dos Estados e

242 À luz do referido diploma, os módulos que deveriam ser ofertados pela Central de Registradores seriam: I - Ofício Eletrônico; II - Penhora Eletrônica de Imóveis (Penhora Online); III - Certidão Digital; IV - Matrícula Online; V - Pesquisa Eletrônica; VI - Protocolo Eletrônico de Títulos (e-Protocolo); VII - Repositório Confiável de Documento Eletrônico (RCDE); VIII - Acompanhamento Registral Online; IX - Monitor Registral; X - Correção Online (Acompanhamento, controle e fiscalização); e XI - Cadastro de Regularização Fundiária Urbana. Essa mesma estrutura se manteve no Serviço de Atendimento Eletrônico Compartilhado (SAEC), com os aperfeiçoamentos e inclusões pertinentes, constituindo o esqueleto do “*front-end*” de todo o Registro Eletrônico de Imóveis.

243 Normas Extrajudiciais da Corregedoria Geral de Justiça de São Paulo: “258. O Serviço de Registro Eletrônico de Imóveis (SREI) será prestado aos usuários externos por meio de plataforma única na *Internet* que funcionará no Portal Eletrônico da Central de Serviços Eletrônicos Compartilhados dos Registradores de Imóveis (Central Registradores de Imóveis), desenvolvido, operado e administrado pela Associação dos Registradores Imobiliários de São Paulo (ARISP) (...)”.

244 Provimento n. 147, de 2015, do CNJ: “Art. 3º. O intercâmbio de documentos eletrônicos e de informações entre os escritórios de registro de imóveis, o Poder Judiciário, a Administração Pública e o público em geral estará a cargo de centrais de serviços eletrônicos compartilhados que se criarão em cada um dos Estados e no Distrito Federal. § 1º. As centrais de serviços eletrônicos compartilhados serão criadas pelos respectivos oficiais de registro de imóveis, mediante ato normativo da Corregedoria Geral de Justiça local.”

Distrito Federal, demandando também a coordenação entre si, para que uniformização da prestação do serviço registral²⁴⁵.

A pulverização das centrais eletrônicas estaduais foi, contudo, contrastada pela necessidade de consolidação de um ponto de acesso universal pela *Internet*, assim como de interoperabilidade inerente às diversas camadas técnicas que envolvem a prestação do serviço registral imobiliário em âmbito nacional.

Aliado à necessidade de prover efetividade à política de regularização fundiária, esse contexto fez surgir no texto da Lei Federal n. 14.365, de 2017, o Operador Nacional do Sistema de Registro Eletrônico de Imóveis (ONR) como responsável por implementar e operar o SREI em âmbito nacional (Tavares, 2018).

O diploma trouxe a estrutura geral para a formação²⁴⁶, sustentação financeira²⁴⁷ e regulação²⁴⁸ do ONR, que seria constituído como entidade privada com vinculação obrigatória de todos os oficiais de registro imobiliário²⁴⁹. Não compõem, assim, a administração pública federal, mas ostenta natureza jurídica *sui generis* (Castro, 2021). Coube à Corregedoria Geral do CNJ editar o Provimento n. 89, de 2019, com as diretrizes específicas para os fins estatutários do ONR e para sua atuação, designando a implantação e operação do Serviço de Atendimento Eletrônico Compartilhado (SAEC) (Castro, 2021).

245 Provimento n. 147, de 2015, do CNJ: “Art. 3º (...). § 2º. Haverá uma única central de serviços eletrônicos compartilhados em cada um dos Estados e no Distrito Federal. (...) § 5º. As centrais de serviços eletrônicos compartilhados coordenar-se-ão entre si para que se universalize o acesso ao tráfego eletrônico e se prestem os mesmos serviços em todo o País”.

246 Lei Federal n. 14.365, de 2017: “Art. 76. (...) 2º O ONR será organizado como pessoa jurídica de direito privado, sem fins lucrativos”.

247 Lei Federal n. 14.365, de 2017: “Art. 76 (...) § 9º Fica criado o fundo para a implementação e custeio do SREI, que será gerido pelo ONR e subvencionado pelas unidades do serviço de registro de imóveis dos Estados e do Distrito Federal referidas no § 5º deste artigo”.

248 Lei Federal n. 14.365, de 2017: “Art. 76. (...) § 4º Caberá à Corregedoria Nacional de Justiça do Conselho Nacional de Justiça exercer a função de agente regulador do ONR e zelar pelo cumprimento de seu estatuto”.

249 Lei Federal n. 14.365, de 2017: “Art. 76. (...) § 5º As unidades do serviço de registro de imóveis dos Estados e do Distrito Federal integram o SREI e ficam vinculadas ao ONR”.

Com o Provimento n. 89, do CNJ, o SREI passa a ser composto por: (i) todos os oficiais de registro de imóveis do Brasil; (ii) o Serviço de Atendimento Eletrônico Compartilhado (SAEC); e (iii) as centrais de serviços eletrônicos compartilhados. Aos poucos, as centrais estaduais perderam protagonismo em relação ao SAEC, que agasalhou de forma horizontal uma gama de atividades implicadas ao registro imobiliário, integralizando serventias extrajudiciais em caráter nacional a partir de um único ponto de acesso na *Internet* (Valério; Benfatti, 2021).

A seu turno, o Provimento n. 180, de 2024, do CNJ, determinou o encerramento das centrais de serviços eletrônicos compartilhados, de gestão dos respectivos Estados e Distrito Federal²⁵⁰, no escopo de concentração da prática registral *online* junto ao SAEC.

A integralização de todas as serventias de registro de imóveis ao SAEC²⁵¹, e a sua prevalência frente à fragmentação das centrais estaduais, deu novos contornos ao SREI. Impulsionou-se a promoção de atos essencialmente digitais, como a emissão de certidões eletrônicas e a recepção de documentos nato-digitais, vinculando uma cadeia complexa de oficiais de Registro de Imóveis à promoção de um novo patamar tecnológico (Miranda, 2023).

Essa convergência de ações para o fomento ao serviço extrajudicial de caráter eletrônico foi consolidada com a Lei Federal n. 14.382, de 2022, que dispôs sobre o Sistema Eletrônico dos Registros Públicos (SERP), com fito de realizar a integralização dos demais escritórios de registros públicos, em moldes da governança semelhantes à coordenação do SREI²⁵².

250 Provimento n. 180, de 2024, do CNJ: “Art. 2º As centrais de serviços eletrônicos compartilhados estaduais e/ou regionais ainda em funcionamento serão desativadas até o dia 30 de junho de 2025”.

251 Importa ressaltar que a integralização de todas as serventias de registro de imóveis ao SAEC foi objeto de normalização promovida pela Corregedoria Nacional do CNJ que, com o seu Provimento n. 124, de 2021, estabeleceu a data de 15 de fevereiro de 2022 como limite para a completude desse processo.

252 A Lei Federal n. 14.382, de 2022, estabeleceu que deveria ser constituído operador nacional, na forma de entidade privada administrada pelos oficiais de registro, conforme regulamentação do CNJ. Com o Provimento n. 139, de 2024, o CNJ trouxe à luz o Operador Nacional do Sistema Eletrônico do Registro Público (ONSERP), composto pelo Operador Nacional do Registro Civil das Pessoas Naturais (ON-RCNP),

O SERP, assim como o SREI em relação ao registro imobiliário, se propõe a construir um sistema eletrônico que efetive a interoperabilidade entre as bases de dados das serventias de registro, sua interconexão e a universalidade do atendimento ao usuário, utilizando-se das estruturas tecnológicas baseadas na *Internet* (Martins, 2022). Para tanto, a construção de parâmetros técnicos, balizados em sólido arcabouço normativo, se mostra essencial para viabilizar um ambiente seguro para o desenvolvimento do registro eletrônico de imóveis.

3. A GOVERNANÇA DE DADOS GEORREFERENCIADOS NO ÂMBITO DO SREI E O USO EM POTENCIAL PELO PODER PÚBLICO MUNICIPAL

O Sistema do Registro Eletrônico de Imóveis, na forma do Provimento n. 89, do CNJ, visa a universalização dos registros imobiliários do Brasil, por meio da interconexão entre as serventias e da interoperabilidade de base de dados. O Provimento n. 195, de 2025, do CNJ trouxe a consolidação dos módulos operacionais do SREI, sendo eles: (i) Central Nacional de Indisponibilidade de Bens (CNIB), (ii) o Serviço de Atendimento Eletrônico Compartilhado (SAEC ou “RI Digital”); (iii) o Inventário Estatístico Eletrônico do Registro de Imóveis (IERI-e); e (iv) o Sistema de Informações Geográficas do Registro de Imóveis (SIG-RI).

Esses módulos se alinham para formulação de um ambiente integrado de serviços inerentes ao registro público de imóveis, conectando oficiais, usuários, gestores públicos e Poder Judiciário, em diferentes aplicações sob gestão do ONR (Martins, 2022). Para fins do

o Operador Nacional do Registro de Títulos e Documentos e Civil das Pessoas Jurídicas (ON-RTDPJ), também nascidos dessa normativa, e o ONR. O Provimento n. 139 teve suas diretrizes inseridas ao Provimento n. 149, de 2023, do CNJ. Nesse ponto, o art. 212, § 2º, desse último, consolidou a estrutura de gestão compartilhada: “A gestão do ONSERP ficará a cargo do Comitê Executivo de Gestão, composto pelos presidentes dos operadores nacionais de registros públicos, que funcionará sob a orientação e a fiscalização da Corregedoria Nacional de Justiça”.

presente estudo, o foco será direcionado ao módulo de Comunicação de Transações Imobiliárias às Prefeituras (CTP), integrante do RI Digital, e ao Sistema de Informações Geográficas do Registro de Imóveis (SIG-RI).

Em ambos os cenários a seguir analisados, o compartilhamento e a integração de dados deve ser pautada na proteção de dados pessoais e na segurança cibernética, por meio de mecanismos eficazes implementados de ponta a ponta da relação, especialmente junto aos municípios, para alcance das recomendações (n. 3.1, 3.2, 3.2.1 e 3.4) inerentes à governança de dados pessoais junto à Carta Brasileira para Cidades Inteligentes.

3.1. A Comunicação de Transações Imobiliárias às Prefeituras, a Resolução n. 547, de 2024, do CNJ, e o SINTER

Com objetivo de aperfeiçoar a atmosfera das execuções fiscais, principalmente da administração pública municipal, o Conselho Nacional de Justiça, editou, em fevereiro de 2024, a sua Resolução n. 547, em que estabelece medidas de integração com o ambiente extrajudicial, em privilégio ao cumprimento da tese fixada junto ao tema n. 1184 de repercussão geral do Supremo Tribunal Federal²⁵³.

Além de autorizar a extinção de execuções fiscais de valor inferior a dez mil reais em certas ocasiões²⁵⁴, a Resolução n. 547 estabelece

253 STF - RE 1355208, Relator(a): CÁRMEN LÚCIA, Tribunal Pleno, julgado em 19/12/2023, Processo Eletrônico Repercussão Geral - Mérito Dje-S/N Divulg. 01/04/2024. Public. 02/04/2024. Tese: “1. É legítima a extinção de execução fiscal de baixo valor pela ausência de interesse de agir tendo em vista o princípio constitucional da eficiência administrativa, respeitada a competência constitucional de cada ente federado. 2. O ajuizamento da execução fiscal dependerá da prévia adoção das seguintes providências: a) tentativa de conciliação ou adoção de solução administrativa; e b) protesto do título, salvo por motivo de eficiência administrativa, comprovando-se a inadequação da medida. 3. O trâmite de ações de execução fiscal não impede os entes federados de pedirem a suspensão do processo para a adoção das medidas previstas no item 2, devendo, nesse caso, o juiz ser comunicado do prazo para as providências cabíveis”.

254 Resolução n. 547, de 2024, do CNJ: “Art. 1º. É legítima a extinção de execução fiscal de baixo valor pela ausência de interesse de agir, tendo em vista o princípio constitucional da eficiência administrativa, respeitada a competência constitucional

condições específicas cumprimento do requisito de interesse processual dessa espécie de demanda (Faim Filho, 2024). Dentre estas, encontram-se a tentativa de conciliação prévia ou adoção de solução administrativa²⁵⁵, bem como a realização de protesto do título²⁵⁶, salvo por motivo comprovado de eficiência administrativa e em outras circunstâncias definidas.

A norma, ademais, consolidou a obrigação de os cartórios de notas e de registro de imóveis enviarem informações de mudanças de titularidades de imóveis, em período não superior a sessenta dias, às prefeituras municipais²⁵⁷. A Resolução visa permitir a atualização cadastral dos contribuintes junto às respectivas Fazendas Municipais, para aperfeiçoar a gestão de tributos e evitar gastos com execuções fiscais malsucedidas.

Regulamentando essa obrigação no âmbito dos cartórios de notas e de imóveis, o Provimento n. 174, de 2024, do CNJ, atribuiu ao ONR o

de cada ente federado. § 1º. Deverão ser extintas as execuções fiscais de valor inferior a R\$ 10.000,00 (dez mil reais) quando do ajuizamento, em que não haja movimentação útil há mais de um ano sem citação do executado ou, ainda que citado, não tenham sido localizados bens penhoráveis” Faim Filho (2024) aponta que o valor de dez mil reais foi escolhido pela norma por ser o valor que mais se aproxima do quantitativo dispendido pela República como custo operacional de uma execução fiscal.

255 Resolução n. 547, de 2024, do CNJ: “Art. 2º. O ajuizamento de execução fiscal dependerá de prévia tentativa de conciliação ou adoção de solução administrativa”.

256 Resolução n. 547, de 2024, do CNJ: “Art. 3º. O ajuizamento da execução fiscal dependerá, ainda, de prévio protesto do título, salvo por motivo de eficiência administrativa, comprovando-se a inadequação da medida. Parágrafo único. Pode ser dispensada a exigência do protesto nas seguintes hipóteses, sem prejuízo de outras, conforme análise do juiz no caso concreto: I – comunicação da inscrição em dívida ativa aos órgãos que operam bancos de dados e cadastros relativos a consumidores e aos serviços de proteção ao crédito e congêneres (Lei nº 10.522/2002, art. 20-B, § 3º, I); II – existência da averbação, inclusive por meio eletrônico, da certidão de dívida ativa nos órgãos de registro de bens e direitos sujeitos a arresto ou penhora (Lei nº 10.522/2002, art. 20-B, § 3º, II); ou III – indicação, no ato de ajuizamento da execução fiscal, de bens ou direitos penhoráveis de titularidade do executado. IV – a inclusão do crédito inscrito em dívida ativa no Cadastro Informativo de créditos não quitados do setor público federal (Cadin) de que trata a Lei nº 10.522/2002”.

257 Resolução n. 547, de 2024, do CNJ: “Art. 4º Os cartórios de notas e de registro de imóveis deverão comunicar às respectivas prefeituras, em periodicidade não superior a 60 (sessenta) dias, todas as mudanças na titularidade de imóveis realizadas no período, a fim de permitir a atualização cadastral dos contribuintes das Fazendas Municipais”.

dever de intermediar essa comunicação em relação aos registradores de imóveis, mediante plataforma que permita aos municípios obterem as informações em único ambiente eletrônico²⁵⁸.

A mudança de titularidade de bens imóveis já era comunicada à Receita Federal, na forma das Declarações de Operações Imobiliárias, em razão do art. 8º da Lei Federal n. 10.426, de 2002²⁵⁹, nas hipóteses previstas atualmente no Instrução Normativa n. 2.186, de 2024²⁶⁰. O Provimento n. 174, do CNJ, regulamentou a sua apresentação às prefeituras, nas mesmas ocasiões em que é exigida à Receita Federal, seguindo o mesmo conteúdo²⁶¹.

258 Provimento n. 149, de 2023, do CNJ: “Art. 184-A. Os cartórios de notas e de registro de imóveis informarão às prefeituras, até o último dia útil do mês subsequente à prática dos atos, todas as mudanças na titularidade de imóveis realizadas no período, a fim de permitir a atualização cadastral dos contribuintes das Fazendas Municipais (art. 4º da Resolução n. 547, de 22/02/2024). (...). § 4º O CNB/CF e o ONR disponibilizarão acesso aos municípios, para obtenção das informações, mediante convênio padronizado, para fins de os destinatários das informações atenderem ao disposto nas regras de proteção de dados e de sigilo fiscal. § 5º O acesso pode ocorrer mediante plataforma que permita aos municípios obterem, em um mesmo ambiente eletrônico, as informações”.

259 Lei Federal n. 10.426, de 2002: “Art. 8º. Os serventuários da Justiça deverão informar as operações imobiliárias anotadas, averbadas, lavradas, matriculadas ou registradas nos Cartórios de Notas ou de Registro de Imóveis, Títulos e Documentos sob sua responsabilidade, mediante a apresentação de Declaração sobre Operações Imobiliárias (DOI), em meio magnético, nos termos estabelecidos pela Secretaria da Receita Federal”.

260 Instrução Normativa n. 2.186, de 2024, da RFB: “Art. 4º Ficam obrigados a apresentar a DOI, sempre que ocorrer operação de aquisição ou alienação de imóvel realizada por pessoa física ou jurídica, independentemente de seu valor, os seguintes serventuários da Justiça, titulares ou designados: (...). II - do Cartório de Registro de Imóveis, quando o documento tiver sido: a) celebrado por instrumento particular; b) celebrado por instrumento particular com força de escritura pública; c) emitido por autoridade judicial, nos casos de adjudicação, herança, legado ou meação; d) decorrente de alienação por iniciativa particular ou mediante leilão judicial; e) assinado pela União, estados, municípios ou Distrito Federal, no âmbito de programas de regularização fundiária ou de programas habitacionais de interesse social; ou f) lavrado pelo Cartório de Notas ou consulados brasileiros, independentemente de ter havido emissão anterior de DOI”.

261 Provimento n. 149, de 2023, do CNJ: “Art. 184-A (...). § 1º As hipóteses de comunicação serão as mesmas objeto das Declarações de Operações Imobiliárias encaminhadas para a Secretaria Especial da Receita Federal do Brasil”.

Para além da ótica de fiscalização tributária e gestão de recursos associados ao litígio administrativo e processual²⁶², o compartilhamento de informações sobre alterações da propriedade imobiliária com órgãos públicos municipais pode fornecer dados para consolidação de políticas públicas baseadas em evidências. Seguindo essa linha, o ONR desenvolveu o módulo de Comunicação de Transações às Prefeituras (CTP) junto ao RI Digital, para centralização da intermediação de dados para com os entes municipais.

Esse módulo permite à administração receber de forma centralizada, automatizada e com espaço de tempo não superior a sessenta dias, informações atualizadas sobre alterações na titularidade dos imóveis registrado, contribuindo para a manutenção do alinhamento de cadastros multifinalitários com a realidade registral, otimizando a governança do solo urbano.

A atualização cadastral de proprietários de imóveis aliada com a adesão ao Sistema Nacional de Gestão de Informações Territoriais (SINTER), cuja alimentação também decorre de serventias extrajudiciais, na forma do art. 2º da Instrução Normativa n. 2.275, de 2025, da Receita Federal²⁶³, representa o potencial de formulação de uma base dados georreferenciada capaz de viabilizar o levantamento informacional para projetos de cidades inteligentes.

262 Pode-se citar como alguns benefícios em relação ao custo da litigiosidade: (i) a redução dos honorários de sucumbências e ônus processuais por extinção da execução fiscal erroneamente ajuizada; (ii) o incentivo à possibilidade de notificação extrajudicial para pagamento da dívida ativa; (iii) a viabilidade do protesto da dívida ativa em cartório e à averbação da certidão da dívida ativa junto à matrícula do imóvel; e (iv) a nomeação adequada de bens ou direitos penhoráveis de titularidade do executado.

263 Instrução Normativa n. 2.275, de 2025, da RFB: “Art. 2º. Os serviços notariais e de registro deverão integrar-se ao Sinter para o compartilhamento de informações e documentos relativos: I - às operações com imóveis previstas no art. 255 da Lei Complementar nº 214, de 16 de janeiro de 2025; e II - aos bens imóveis registrados, para fins de apuração de seu valor de referência”. Na forma do art. 255, da LCp n. 214, de 2025, são essas as operações mencionadas na IN: “I - da operação de alienação do bem imóvel; II - da locação, cessão onerosa ou arrendamento do bem imóvel; III - da cessão ou do ato oneroso translativo ou constitutivo de direitos reais sobre bens imóveis; IV - da operação de administração ou intermediação; V - da operação nos serviços de construção civil”.

Contextualizando com a proposta metodológica de Justi (2021), o SINTER viabiliza a rotulação de bens imóveis de características especiais (BICE), que servem à identificação de elementos integrantes do patrimônio dos entes federativos (Gruber, 2016), e bens públicos ou privados de uso especial, na forma do Decreto n. 11.208 de 2012:

Art. 3º. Para fins do disposto neste Decreto, considera-se:

(...)

XII - Bens Imóveis de Características Especiais - BICE - bens públicos ou privados de uso especial e os bens do patrimônio cultural integrantes do domínio da União, dos Estados, do Distrito Federal e dos Municípios, incluído o espaço aéreo sobre esses bens, o subsolo e as áreas do mar territorial, da zona econômica exclusiva e da plataforma continental, como:

- a) usinas nucleares, hidrelétricas e termoeletricas;
- b) parques eólicos e plantas solares;
- c) plataformas, sondas de prospecção e plantas de refino de petróleo e gás;
- d) portos, eclusas, aeroportos e terminais rodoviários, ferroviários e hidroviários;
- e) aquedutos, gasodutos e minerodutos;
- f) aquíferos e jazidas minerais;
- g) rodovias, estradas, vias vicinais, túneis, pontes e viadutos;
- h) praças e logradouros;
- i) museus, prédios, monumentos históricos e sítios arqueológicos;
- j) terras indígenas e terras devolutas;
- k) lagos, lagoas, rios, quedas-d'água, reservatórios de barragens, açudes, cursos-d'água navegáveis, mananciais e espelhos-d'água; e
- l) parques, florestas, áreas ambientais e unidades de conservação.

A comunicação de transações de propriedade imobiliária e os registros do SINTER podem contribuir para a formulação de Cadastro Territorial Multifinalitário (CTM), na forma da Portaria n. 3.242, de

2022, do Ministério do Desenvolvimento Regional, junto à respectiva administração municipal.

Esse contexto contribui para alcance de objetivos estratégicos da Carta Brasileira para Cidades Inteligentes, quanto às recomendações inerentes à consolidação de cadastros multifinalitários (n. 1.5.1.5), e à interoperabilidade a nível de dados (n. 3.4, 3.5.1 e 3.8), na medida em que viabiliza a qualidade e relevância da base de dados dos órgãos municipais, privilegiando a gestão territorial integrada e georreferenciada.

3.2. O Provimento n. 195, de 2025, do CNJ, e a governança de dados georreferenciados no SREI

Em junho de 2025, o Conselho Nacional de Justiça editou o seu Provimento n. 195, que inseriu no Código Nacional de Normas do Foro Extrajudicial (Provimento n. 149, de 2023) diretrizes específicas para o adequado controle da malha imobiliária, da disponibilidade e da unicidade matricial, mediante implementação de um Sistema de Informações Geográficas (SIG) que permita aos oficiais de registro de imóveis a verificação da exata localização e descrição dos imóveis georreferenciados, formando um mosaico.

Fundamentalmente, o Provimento n. 149, do CNJ, estabeleceu dois novos módulos no SREI: o Inventário Estatístico Eletrônico do Registro de Imóveis (IERI-e), conceituado como a base de dados estatísticos do registro de imóveis²⁶⁴, e o Sistema de Informações Geográficas do Registro de Imóveis (SIG-RI), institucionalizado como a base de dados geográficos relativos às informações imobiliárias mantidas pelos cartórios de registro de imóveis²⁶⁵.

264 Provimento n. 149, de 2023, do CNJ: “Art. 343-A. O Inventário Estatístico Eletrônico do Registro de Imóveis (IERI- e) é um módulo operacional do Sistema de Registro Eletrônico de Imóveis (SREI) destinado a servir de base de dados estatísticos do registro de imóveis, sob a gestão e manutenção do Operador Nacional do Sistema de Registro Eletrônico de Imóveis (ONR)”.

265 Provimento n. 149, de 2023, do CNJ: “Art. 343-D. O Sistema de Informações Geográficas do Registro de Imóveis (SIG-RI) destina-se a servir de base de dados

Na forma designada pela norma, o SIG-RI deve ser alimentado pelos oficiais de registro de imóveis, quando da prática de atos registrais em matrículas cujo imóvel já esteja georreferenciado²⁶⁶, e nos casos em que há obrigação desse procedimento ser feito, mantendo-se a interoperabilidade com sistemas de governança fundiária²⁶⁷, como o SINTER e o Sistema de Gestão Fundiária do INCRA (SIGEF).

A obrigação de georreferenciamento de imóveis rurais, nas hipóteses de desmembramento, parcelamento ou remembramento, tem por fundamento o § 3º do art. 176, da Lei de Registros Públicos²⁶⁸,

geográficos relativos às informações imobiliárias mantidas pelos cartórios de registro de imóveis”.

266 Provimento n. 149, de 2023, do CNJ: “Art. 343-F. Compete aos oficiais de registro de imóveis a adoção das seguintes medidas, em relação aos imóveis rurais georreferenciados e certificados pelo Sigef e aos urbanos: I - alimentar o SIG-RI com os perímetros dos imóveis georreferenciados e, no caso dos rurais, certificados pelo Sigef obtidos a partir da descrição constante da matrícula, a fim de formar o mosaico dos imóveis registrados com coordenadas geodésicas; II - quando da prática de atos que envolvam a abertura de matrícula ou a atualização, a correção ou a alteração da descrição perimetral do imóvel, analisar o mosaico registral criado no SIG-RI, a fim de verificar a ocorrência de alguma das situações abaixo: a) descrição perimétrica que apresente coordenadas polares com erros de fechamento do polígono (erro na descrição do polígono); b) sobreposições de área com outros imóveis; III - quando da prática de qualquer ato na matrícula, valer-se do SIG-RI para averiguar a existência de irregularidade de especialidade objetiva em relação a outras matrículas, salvo se tal averiguação já tiver sido realizada anteriormente na forma do § 3º, do art. 440-AQ deste Código: a) controle da malha imobiliária, mediante a disponibilização e a análise das informações geográficas dos imóveis cuja descrição no fólio real contenha coordenadas georreferenciadas; b) controle de disponibilidade, por meio da alimentação e a análise dos indicadores reais, impedindo registros de imóveis em duplicidade material de matrículas e alienações a *non domino*; c) controle da unicidade matricial, com a abertura de apenas uma matrícula para cada imóvel, mediante a conferência das anotações de encerramento/destaque dos registros anteriores das matrículas dos imóveis objeto de georreferenciamento”.

267 Provimento n. 149, de 2023, do CNJ: “Art. 343-D. (...). § 3º. O SIG-RI deverá manter interoperabilidade entre os registros de imóveis e os sistemas de governança fundiária, nos termos de manual técnico do ONR”.

268 Lei Federal n. 6.015, de 1973: “Art. 176. O Livro nº 2 - Registro Geral - será destinado, à matrícula dos imóveis e ao registro ou averbação dos atos relacionados no art. 167 e não atribuídos ao Livro nº 3. § 1º. A escrituração do Livro nº 2 obedecerá às seguintes normas: (...) II - são requisitos da matrícula: (...) 3) a identificação do imóvel, que será feita com indicação: a - se rural, do código do imóvel, dos dados constantes do CCIR, da denominação e de suas características, confrontações, localização e área; b - se urbano, de suas características e confrontações, localização, área, logradouro, número e de sua designação cadastral, se houver. (...). § 3º. Nos casos de desmembramento, parcelamento ou remembramento de imóveis rurais, a identificação prevista na alínea

com redação dada pela Lei Federal n. 10.267, de 2001. O Provimento n. 195, do CNJ, disciplinou, por sua vez, essa obrigatoriedade, por ocasião de abertura de matrícula, em relação aos imóveis urbanos quando de requerimento do interessado e nos casos de regularização fundiária urbana²⁶⁹, na forma da Lei Federal n. 13.465, de 2017²⁷⁰.

Essa legislação já previa, inclusive, o dever de o Poder Público apresentar planta²⁷¹ e memorial descritivo²⁷² de área objeto de regularização mediante coordenadas georreferenciadas, no procedimento de demarcação urbanística²⁷³. De mesma sorte, o

a do item 3 do inciso II do § 1º será obtida a partir de memorial descritivo, assinado por profissional habilitado e com a devida Anotação de Responsabilidade Técnica – ART, contendo as coordenadas dos vértices definidores dos limites dos imóveis rurais, geo-referenciadas ao Sistema Geodésico Brasileiro e com precisão posicional a ser fixada pelo INCRA, garantida a isenção de custos financeiros aos proprietários de imóveis rurais cuja somatória da área não exceda a quatro módulos fiscais”.

269 Provimento n. 149, de 2023, do CNJ: “Art. 440-AQ. Além das informações obrigatórias constantes do art. 176, II, da Lei n. 6.015/1973, por ocasião do ato de abertura, a matrícula deverá conter: (...) III - a descrição perimetral mediante georreferenciamento para: a) os imóveis rurais, com obrigatoriedade de prévia certificação da poligonal no INCRA, na forma dos § 3.º a 5.º do art. 176 da Lei n. 6.015/1973; b) os demais imóveis rurais, caso em que a certificação da poligonal no INCRA é facultativa, a critério do interessado; e c) os imóveis urbanos nas seguintes hipóteses: 1) requerimento do interessado; 2) regularização fundiária urbana (Reurb)”.

270 Discute-se, ainda a obrigatoriedade de georreferenciamento de imóveis urbanos para fins de regularidade do Cadastro Imobiliário Brasileiro (CIB), a teor do art. 14 da Instrução Normativa n. 2.030, de 2021, da RFB: “Art. 14. A inscrição no CIB será considerada irregular quando for constatada: I - inconsistência na identificação do proprietário, titular do domínio útil ou possuidor a qualquer título; II - sobreposição de geometrias; III - ausência de dados georreferenciados; ou IV - outras inconsistências nos dados cadastrais”. Outro relevante argumento a favor do georreferenciamento dos imóveis urbanos consiste no § 1º do art. 29 do Decreto n. 9.310, de 2018, que prevê que “Os limites das unidades imobiliárias serão definidos por vértices georreferenciados ao Sistema Geodésico Brasileiro”, sem distinção ou vinculação à regularização urbana (Mallmann *et al.*, 2024).

271 Conforme Mallmann *et al.* (2024, p. 241), a planta do perímetro do núcleo urbano é o complemento do levantamento planialtimétrico, e o perímetro é a linha que forma o contorno da gleba, caracterizada pela soma de seus lados.

272 “Os memoriais descritivos são a representação escrita das medidas, características, confrontações e localização dos imóveis. Têm por finalidade caracterizar criteriosamente as unidades imobiliárias (lotes ou terrenos), detalhando-se todos os elementos necessários à identificação do imóvel, isto é, dando-se certeza do seu objeto” (Mallmann *et al.*, 2024, p. 245).

273 Lei Federal n. 13.465, de 2017: “Art. 19. O poder público poderá utilizar o procedimento de demarcação urbanística, com base no levantamento da situação

projeto de regularização fundiária deve conter o levantamento planialtimétrico²⁷⁴ e cadastral, com georreferenciamento²⁷⁵.

O georreferenciamento permite ao Poder Público conhecer de forma precisa a realidade do núcleo a ser regularizado, oferecendo dados consistentes para a formulação da política de regularização e assegurando os limites dos imóveis envolvidos (Mallmann *et al.*, 2024).

A aposição de coordenadas geodésicas na descrição de bens imóveis junto ao registro constitui, portanto, obrigação que abrange os bens imóveis situados em área urbana, especialmente em locais que estão sendo ou já foram objeto de regularização fundiária urbana. Esse processo ocorre com fundamento técnico na NBR ABNT 17047:2022, que estabelece os procedimentos para a adequada descrição dos imóveis urbanos, com base no georreferenciamento ao Sistema Geodésico Brasileiro das coordenadas dos vértices dos limites do imóvel com precisão posicional definida (Mallmann *et al.*, 2024).

O SIG-RI possui como plataforma gráfica o Mapa do Registro de Imóveis²⁷⁶, que pretende, entre outras funções, viabilizar

da área a ser regularizada e na caracterização do núcleo urbano informal a ser regularizado. § 1º O auto de demarcação urbanística deve ser instruído com os seguintes documentos: I - planta e memorial descritivo da área a ser regularizada, nos quais constem suas medidas perimetrais, área total, confrontantes, coordenadas georreferenciadas dos vértices definidores de seus limites, números das matrículas ou transcrições atingidas, indicação dos proprietários identificados e ocorrência de situações de domínio privado com proprietários não identificados em razão de descrições imprecisas dos registros anteriores; II - planta de sobreposição do imóvel demarcado com a situação da área constante do registro de imóveis”.

274 Conforme Mallmann *et al.* (2024, p. 235), “o levantamento planialtimétrico é um documento que descreve a gleba ou terreno com exatidão, no qual são anotados medidas planas, ângulos e diferenças de nível ou inclinação”.

275 Lei Federal n. 13.465, de 2017: “Art. 35. O projeto de regularização fundiária conterá, no mínimo: I - levantamento planialtimétrico e cadastral, com georreferenciamento, subscrito por profissional competente, acompanhado de Anotação de Responsabilidade Técnica (ART) ou Registro de Responsabilidade Técnica (RRT), que demonstrará as unidades, as construções, o sistema viário, as áreas públicas, as acidentes geográficos e os demais elementos caracterizadores do núcleo a ser regularizado”.

276 Provimento n. 149, de 2023, do CNJ: “Art. 343-D. (...) § 2º. O Mapa do Registro de Imóveis do Brasil (Mapa) é a ferramenta do SIG-RI destinada a servir como plataforma gráfica dos imóveis registrados nos cartórios de registro de imóveis, de modo a, entre outras finalidades: I – viabilizar consultas públicas; II – permitir a análise e gestão dos processos de georreferenciamento em relação aos imóveis registrados; III – permitir interações com outros bancos de dados que possuam coordenadas geodésicas; IV –

consultas públicas, permitir a análise e gestão dos processos de georreferenciamento em relação aos imóveis registrados; e permitir interações com outros bancos de dados que possuam coordenadas geodésicas, como o Cadastro Territorial Multifinalitário.

Os sistemas de coordenadas geodésicas, quando integrados a cadastros multifinalitários, tornam-se ferramentas estratégicas para políticas públicas de gestão do solo urbano, de regularização da moradia e preservação do meio ambiente (Gruppi; Sanches, 2025). Nesse sentido, a matrícula passa de um aspecto individual para fornecer informações essenciais à gestão de bens públicos e organização da política urbana.

A consolidação gráfica dessas informações pode ser integrada com o Cadastro Territorial Multifinalitário a que se refere Portaria MDR n. 3.242, de 2022, que é orientado pelas coordenadas dos vértices de limite vinculadas ao sistema geodésico brasileiro²⁷⁷, com privilégio às parcelas certificadas²⁷⁸. A visualização gráfica de elementos do solo urbano, a integração entre cadastros oficiais, e obrigatoriedade de associação de bens imóveis a coordenadas geodésicas para a prática de atos registrais, se associa com o levantamento de informações basilares à condução de projetos de cidades inteligentes.

permitir a identificação de eventual sobreposição, total ou parcial, de poligonais de matrículas, com acesso a, no mínimo, estas informações: a) área do imóvel objeto da matrícula; b) área do imóvel em sobreposição; c) área, perímetro e porcentagem da sobreposição existente; V – alertar automaticamente possíveis casos de sobreposição ou vácuo dominial entre imóveis que ultrapassem os limites das tolerâncias posicionais normatizadas, conforme manual técnico do ONR”.

277 Portaria n. 3.242, de 2022, do MDR: “Art. 4º. A parcela é a representação de uma porção territorial de extensão contínua. São elementos da parcela: I - as coordenadas dos vértices de limite vinculadas ao sistema geodésico brasileiro; II - o código de identificação único, inequívoco e estável; III - os direitos individuais e coletivos que a originam; e IV - os identificadores que possibilitem o relacionamento com os cadastros temáticos”.

278 Portaria n. 3.242, de 2022, do MDR: “Art. 5º. Para fins de aperfeiçoamento do cadastro territorial, a parcela pode ser caracterizada como certificada ou não certificada. § 1º. Parcela certificada é aquela cujos limites foram obtidos com apoio geodésico e com precisão estabelecida em norma específica, representando os limites legais ou de fato para que torne possível levá-la a registro. (...) § 6º. As parcelas certificadas devem progressivamente substituir as não certificadas”.

Observa-se que esse contexto técnico-normativo contribui para alcance de objetivos estratégicos da Carta Brasileira para Cidades Inteligentes quanto às recomendações inerentes à consolidação de cadastros multifinalitários (n. 1.5.1.5), ao uso de ferramentas de geoprocessamento para diagnóstico e gestão urbana (n. 1.5.1.1), à interoperabilidade a nível de dados (n. 3.5.1 e 3.8), e ao fortalecimento da infraestrutura nacional de dados espaciais (n. 3.5.2), na medida em que viabilizam a elaboração, registro/certificação e integração de dados georreferenciados, que podem ser utilizados na formulação de políticas públicas de eficiência estratégica no ambiente urbano.

CONSIDERAÇÕES FINAIS

Ao longo da presente pesquisa, foram analisados os aspectos inerentes à governança de dados, à interoperabilidade de sistemas e ao georreferenciamento de informações no contexto da Agenda Brasileira para Cidades Inteligentes. Foi possível identificar que esses temas estruturam recomendações para alcance de diversos eixos, como o objetivo n. 1 – “integrar a transformação digital nas políticas, programas e ações de desenvolvimento urbano sustentável, respeitando as diversidades e considerando as desigualdades presentes nas cidades brasileiras”, e o objetivo n. 3 – “estabelecer sistemas de governança de dados e de tecnologias, com transparência, segurança e privacidade”.

Para a construção de projetos de cidades inteligentes, a governança de dados, que consiste em mecanismos de interoperabilidade, segurança cibernética e proteção de dados pessoais, e o georreferenciamento, atinente à qualidade, relevância e representação gráfica de registros administrativos e dados de cadastros territoriais, possuem importância singular, de maneira que a Carta optou por estabelecer recomendações específicas para sua implementação por órgãos municipais, na esteira da agenda pública.

Ao se investigar o desenvolvimento normativo do Sistema do Registro Eletrônico de Imóveis (SREI), para compreensão da sua relação

com informações potencialmente úteis para cidades inteligentes, pôde-se compreender que seu delineamento não foi uniforme, previsível e sistematizado desde a sua concepção na Lei Federal n. 11.977, de 2009. O seu desenvolvimento decorreu de um conjunto normas que sucessivamente foram dando estrutura e modelando a atividade.

Observou-se que o SREI, no formato atual, apresenta uma sólida estrutura de governança e sustentabilidade que viabiliza a sua operação em âmbito nacional, interconectando serventias de registro imobiliário de todo o país, e interoperando com órgãos públicos, e Poder Judiciário, concentrando a prestação digital dos serviços em único ponto de acesso na *Internet*, o Serviço de Atendimento Eletrônico Compartilhado (“RI Digital”).

No campo da interoperabilidade de sistemas e da governança de dados, verificou-se que o módulo de Comunicação de Transações Imobiliárias às Prefeituras (CTP), integrante do RI Digital, apresenta estrutura e exigibilidade semelhantes às Declarações de Operações Imobiliárias (DOI). Esse módulo constitui uma fonte robusta de informações estruturadas e constantemente atualizadas sobre a propriedade de imóveis. Esses dados podem ser integrados ao cadastro territorial multifinalitário, que serve de base para políticas públicas orientadas por evidências, especialmente nas áreas de regularização do solo urbano, sustentabilidade e eficiência em cidades inteligentes.

A seu turno, o georreferenciamento está inserido no módulo do Sistema de Informações Geográficas do Registro de Imóveis, conforme dispõe o Provimento n. 195, de 2025, do CNJ. Esse provimento representa um avanço significativo para a governança de dados no registro imobiliário brasileiro. A norma estabelece a integração entre cartórios e cadastros de governança territorial, fundiária e multifinalitários.

Nessa lógica, a matrícula passa a ser instrumento de informação estratégica, capaz de sustentar o planejamento territorial e o desenvolvimento social, ambiental e econômico. Esse processo se insere no contexto de projetos de cidades inteligentes, em consonância com as recomendações da Carta Brasileira para Cidades Inteligentes.

REFERÊNCIAS

ACIOLY, Luis Henrique de Menezes; SILVA, Matheus Fernandes da; MONTEIRO NETO, João Araújo. A Emenda Constitucional nº 115 de 10 de fevereiro de 2022 e o *enforcement* da proteção de dados pessoais no Brasil. *Revista de Investigações Constitucionais*, v. 11, n. 3, p. e275, 2024. Disponível em: <https://revistas.ufpr.br/rinc/article/view/92117>. Acesso em: 20 ago. 2025.

ANTONIALLI, Dennys Marcelo; KIRA, Beatriz. Planejamento Urbano do Futuro, Dados do Presente: A proteção da Privacidade no Contexto das Cidades Inteligentes. *Revista Brasileira de Estudos Urbanos e Regionais*, v. 22, E202003, 2020. Disponível em: <https://doi.org/10.22296/2317-1529.rbeur.202003>. Acesso em: 15 out. 2024.

ASSAD, Frederico Jorge Vaz de Figueiredo. Registro de imóveis eletrônico e governança fundiária. *Revista de Direito Imobiliário*, a. 39, v. 81, p. 215-234, jul./dez. 2016.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. *Radar Tecnológico: Cidades Inteligentes*. Vol. 1. Brasília: ANPD, 2024.

BELLI, Luca; DONEDA, Danilo. Governança de Dados nas “Cidades Inteligentes”: Ensinaamentos aprendidos das práticas brasileiras e europeias. In: REIA, Jess; BELLI, Luca (orgs). *Smart Cities no Brasil: regulação, tecnologia e direitos*. Belo Horizonte: Casa do Direito, 2021, p. 61-91.

BERNDSSEN, Guilherme Rigo. *A operação urbana consorciada como instrumento de urbanismo sustentável*. Dissertação (Mestrado em Ciência Jurídica) - Universidade do Vale de Itajaí (UNIVALI), Itajaí, 2019.

BIONI, Bruno Ricardo. *Regulação e Proteção de Dados Pessoais: O Princípio da Accountability*. Rio de Janeiro: Forense, 2022.

BRUNO, Ana Paula *et al.* Carta Brasileira para Cidades Inteligentes – produto e processo de construção de uma agenda pública para a transformação digital nas cidades. In: JÚNIOR, Franciso (Coord); CARNEIRO, Leandro *et al* (orgs). *Cidades Inteligentes: Uma abordagem sustentável*. Brasília: Câmara dos Deputados, 2021, p. 175-189.

CASTELLS, Manuel. *A sociedade em rede*. Trad. Roneide Venâncio Majer. 6. ed. São Paulo: Paz e Terra, 2002.

CASTRO, Manuella Santos. *Registro de Imóveis na Era Digital: Impactos das novas tecnologias no sistema registral brasileiro*. 2021, 306 f. Tese (Doutorado) - Faculdade de Direito, Universidade de São Paulo, São Paulo, 2021.

CHEZZI, Bernardo. A aplicação da LGPD ao Registro de Imóveis. In: GALHARDO, F.; PARO, J. P.; NALINI, J. R.; BRANDELLI, L. (org). *Direito Registral e Novas Tecnologias*. Rio de Janeiro: Forense, p. 139-167, 2021.

DUARTE, Fábio. Cidades Inteligentes: Inovação Tecnológica no meio urbano. *São Paulo em Perspectiva*, v. 19, n. 1, p. 122-131, jan./mar. 2005.

FAIM FILHO, Eurípedes Gomes. Tema 1.184 do STF e Resolução 547 do CNJ: algumas observações de ordem jurídica. *Cadernos Jurídicos*, São Paulo, ano 25, nº 67, p. 46-51, jan.-mar. 2024.

FALEIROS JÚNIOR, José Luiz de Moura. Inovação, desenvolvimento e a Lei do Governo Digital (Lei nº 14.129/2021): perspectivas quanto às estruturas de governo como plataforma. *Inova Jur - Revista Jurídica da UEMG*, Belo Horizonte, v. 1, n. 1, p. 1-29, jan./jun. 2022.

FALEIROS JÚNIOR, José Luiz de Moura. Planejamento Urbano e Tecnologia: Potencialidades para o Implemento de Cidades Inteligentes no Brasil. In: GORDILHO, Heron *et al.* (Coords). *Administração pública, meio ambiente e tecnologia*. II Congresso Internacional de Direito, Políticas Públicas, Tecnologia e Internet. Franca: Faculdade de Direito de Franca, 2024, p. 113-120.

FIORANELLI, Ademar. Matrícula no registro de imóveis: questões práticas. In: YOSHIDA, Consuelo Yatsuda Moromizato Yoshida; FIGUEIREDO, Marcelo. AMADEI, Vicente de Abreu (coords). *Direito notarial e registral avançado*. São Paulo: Revista dos Tribunais, 2014.

GIL, Antonio Carlos. *Como Elaborar Projetos de Pesquisa*. 4 ed. São Paulo: Atlas, 2002.

GRUBER, Rafael Ricardo. Registro Eletrônico de Imóveis, Cadastros e SINTER: Interconexão sem Submissão. *Revista de Direito Imobiliário*, a. 39, v. 81, p. 253-287, jul./dez. 2016.

GRUPPI, Bruno Drumond; SANCHES, Luiz Antonio Mano Ugeda. A matrícula como serviço: O que muda com o provimento CNJ 195/25. *Migalhas*, 2 set. 2025. Disponível em: <https://www.migalhas.com.br/depeso/439072/a-matricula-como-servico-o-que-muda-com-o-provimento-cnj-195-25>. Acesso em: 20 set. 2025.

HENRIQUES, Antonio; MEDEIROS, João Bosco. *Metodologia Científica da Pesquisa Jurídica*. 9. ed. São Paulo: Atlas, 2017.

JUSTI, Alexander Rodrigues. Melhoria da gestão das cidades através do uso de modelo CIM 3D. In: JÚNIOR, Francisco (Coord); CARNEIRO, Leandro *et al.* (orgs). *Cidades Inteligentes: Uma abordagem sustentável*. Brasília: Câmara dos Deputados, 2021, p. 203-214.

KOMNINOS, Nicos. Intelligent cities: towards interactive and global innovation environments. *Int. J. Innovation and Regional Development*, v. 1, n. 4, p. 338-335, 2009.

LIM, Chiehyeon; KIM, Kwang-Jae; MAGLIO, Paul P. Smart cities with big data: Reference models, challenges, and considerations. *Cities*, v. 82, p. 86-99, 2018. Disponível em: <https://doi.org/10.1016/j.cities.2018.04.011>. Acesso em: 10 ago. 2025.

LIMA, Gabriel Ribeiro. *Cidade “inteligente” (smart city): entre o direito urbanístico e a proteção dos dados pessoais*. 2024. 163 f. Dissertação (mestrado) - Universidade Federal de Minas Gerais, Faculdade de Direito, Belo Horizonte, 2024.

MADALENA, Juliano. Regulação das Fronteiras da Internet: um primeiro passo para uma Teoria Geral do Direito Digital. In: MARTINS, G. M.; LONGHI, J. V. R. (coords.). *Direito Digital: Direito Privado e Internet*. 2. ed. Indaiatuba: Foco, 2019. p. 183-206.

MAIA, Erica Von Raschendorfer Bastos; FIGUEIRA, Ariane Cristine Roder. Cidades inteligentes sob a ótica do direito à cidade: revisão de literatura e proposta de framework conceitual. *Revista da EMERJ*, v. 26, p. 1-18, 2024. Disponível em: <https://ojs.emerj.com.br/index.php/revistadaemerj/article/view/610>. Acesso em: 15 mar. 2025.

MALLMANN, Jean Karlo Woiciechoski; TEIXEIRA, Aparecida Netto; MOURAD, Laila Nazem. Reurb: do georreferenciamento na regularização fundiária urbana. *Revista Brasileira de Direito Urbanístico – RBDU*, Belo Horizonte, a. 10, n. 18, p. 231-256, jan./jun. 2024.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. *Técnicas de Pesquisa*. 9. Ed. São Paulo: Atlas, 2021.

MARTINS, Ricardo Anderson Rios de Souza. *A tecnologia no âmbito do registro de imóveis como instrumento da solidariedade na concretização da dignidade humana, no processo das intersecções jurídicas entre o público e o privado derivado do constitucionalismo contemporâneo brasileiro*. 2024, 140 f. Dissertação (Mestrado em Direito) - Universidade de Santa Cruz do Sul, 2024.

MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. *Big Data, como extrair volume, variedade e valor*. Trad. Paulo Polzonoff Junior. Rio de Janeiro: Elsevier, 2013.

MINISTÉRIO DO DESENVOLVIMENTO REGIONAL. *Carta Brasileira para Cidades Inteligentes*. Ed. Rev. Brasília, 2021.

MIRANDA, Caleb Matheus Ribeiro de. Comentários ao Sistema Eletrônico de Registros Públicos (SERP) – artigos 1º ao 9º. In: KÜMPEL, Vitor (Coord). *Breves comentários à Lei nº 14.382/2022*. 2 ed. São Paulo: YK, 2023, p. 11-48.

NAZARENO, Cláudio. As cidades inteligentes, o controle dos dados e a questão pessoal. In: JÚNIOR, Francisco (Coord); CARNEIRO, Leandro *et al.* (orgs). *Cidades Inteligentes: Uma abordagem sustentável*. Brasília: Câmara dos Deputados, 2021, p. 301-311.

O'REILLY, Tim. Government as platform. *Innovations: Technology, Governance, Globalization*, Cambridge, v. 6, n. 1, p. 13-40, 2011. Disponível em: <https://direct.mit.edu/itgg/article/6/1/13/9649/Government-as-a-Platform>. Acesso em: 15 jun. 2024.

RIBEIRO, Moacyr Petrocelli de Ávila. A Matrícula: Paradigmas para o Sistema do Registro Eletrônico de Imóveis. *Revista de Direito Imobiliário*, a. 42, v. 86, p. 215-262, jan./jun. 2019.

SOUSA JÚNIOR, Almir Mariano *et al.* *Carta Brasileira para Cidades Inteligentes: Versão Resumida*. São Paulo: Livraria da Física, 2021.

TAVARES, Ramos André. O Operador Nacional do Sistema de Registro Eletrônico de Imóveis: Resposta à Exigência Constitucional de um Eficiente Sistema Registral. *Jornal Eletrônico Migalhas*, v. 136, p. 23-42, 2018. Disponível em: <https://www.migalhas.com.br/arquivos/2018/8/art20180821-03.pdf>. Acesso em: 01. jul. 2024.

VALERIO, Alexandre Scigliano; BONFATTI, Fabio Fernandes Neves. Possibilidade de Assinatura, Registro e Protesto Eletrônico dos Títulos de Crédito do Agronegócio. *Revista Brasileira de Direito Empresarial*, v. 7, n. 2, p. 17-38, jul./dez. 2021.

9. SANDBOXES REGULATÓRIOS E A PROTEÇÃO DOS DADOS PESSOAIS OBTIDOS EM AMBIENTES EXPERIMENTAIS

George José Nascimento de Souza

Advogado tributarista no escritório Manzi Advogados em Recife e atendendo a quatro outros estados do Nordeste, no Rio de Janeiro, São Paulo e Brasília. Formado na Universidade Católica de Pernambuco, MBA em Direito da Economia e da Empresa pela FGV, Especialista em Direito Marítimo e Portuário pela Universidade Maurício de Nassau/Escola Superior de Advocacia da OAB/PE e Especialista em Direito Processual Tributário na Universidade Federal de Pernambuco. Especialista em Direito Digital pelo Instituto de Tecnologia e Sociedade do Rio de Janeiro – ITS Rio em parceria com o Centro de Estudos e Pesquisas no Ensino do Direito da Universidade do Estado do Rio de Janeiro (CEPED/UERJ).

INTRODUÇÃO

Há um postulado, criado por Gordon Moore (cofundador da Intel), conhecido como “Lei de Moore”, que afirma que o número de transistores (poder computacional) dobraria anualmente. Em 1965, Moore (2005) afirmou que a complexidade para os custos mínimos de componentes tem aumentado a uma taxa de aproximadamente um fator de dois por ano (ver gráfico na próxima página). Certamente, a curto prazo, espera-se que essa taxa continue, se não aumentar. A longo prazo, a taxa de aumento é um pouco mais incerta, embora não haja razão para acreditar que não permanecerá quase constante por pelo menos 10 anos.

Dez anos depois, Moore revisou sua previsão e afirmou que o poder computacional dobraria a cada dois anos. Apesar da revisão da periodicidade, esse postulado demonstra como a tecnologia avança de forma exponencial e muito mais rápida do que a legislação e a regulação normativa de qualquer País poderia alcançar.

Diante desse avanço implacável, foi necessário conceber um instrumento jurídico que possibilitasse aos agentes públicos meios para mitigar os riscos dessas novas tecnologias ao interesse público, bem como para evitar a criação de barreiras burocráticas desnecessárias que resultassem em travas ao desenvolvimento tecnológico local e nacional.

Isto é, a tecnologia não poderia ser vista exclusivamente como um perigo do qual é necessário proteger a sociedade, impedindo a inovação e o avanço tecnológico, bem como não poderia ser tratada como um instrumento que não representasse qualquer risco à população, caso utilizada sem qualquer limitação pelos seus agentes.

A partir dessas necessidades foi concebido um mecanismo que permite o acesso a um ambiente controlado para empresas e entidades pudessem testar os seus serviços e produtos, onde haveria um relaxamento ou até mesmo suspensão dos limites regulatórios, reduzindo sensivelmente os riscos dessas tecnologias para a população local.

O ambiente regulatório experimental é mais conhecido pelo anglicismo *sandbox* regulatório, uma ferramenta jurídica que possibilita o Gestor Público incentivar e estimular a produção e criação de novas tecnologias em um ambiente controlado, através de benefícios e incentivos fiscais e relaxamento de salvaguardas e obrigações regulatórias; estabelecendo metas e objetivos para o empreendedor que pretenda inovar e testar novos produtos e serviços.

Esse tipo de instrumento tem origem nos conceitos próprios da computação de ambientes onde os programadores testam as aplicações antes de disponibilizarem para o público-alvo e, antes disso, inspirado no ambiente seguro onde as crianças podem brincar em parques sem risco (caixa de areia). Ele foi utilizado pela primeira vez no setor de serviços financeiros, onde os primeiros arcabouços jurídicos que tratavam sobre o tema foram concebidos nos Estados Unidos em 2012

e no Reino Unido em 2015, quando o termo foi cunhado (*regulatory sandbox*).²⁷⁹

Em outras palavras, *sandboxes* regulatórios criam espaços onde as autoridades públicas interagem com pessoas físicas ou jurídicas para testar produtos ou serviços inovadores que desafiam os marcos legais existentes. Os agentes participantes obtêm dispensa de disposições legais específicas ou de processos de conformidade, permitindo-lhes inovar. As abordagens aos *sandboxes* regulatórios variam, mas compartilham características comuns: são temporários, com um processo de teste geralmente limitado a seis meses; reúnem reguladores e empresas; dispensam disposições legais existentes e oferecem suporte jurídico personalizado para um projeto específico, frequentemente com base em tentativa e erro; além disso, as informações técnicas, de mercado e os dados coletados auxiliam as autoridades regulatórias a avaliar se os marcos legais existentes são adequados ou precisam ser adaptados (OCDE, 2023).

Desde a sua implementação no Brasil através da Lei Federal nº. 13.874 de 20 de setembro de 2019, que instituiu a Declaração Direitos de Liberdade Econômica, autorizando as pessoas privadas a desenvolver, executar, operar e/ou comercializar novas modalidades de produtos e de serviços, mesmo quando as normas infralegais se mostrem desatualizadas por força de desenvolvimento tecnológico consolidado internacionalmente (BRASIL, 2019); seguida pela Lei Complementar nº. 182 de 1º de junho, que instituiu o Marco Legal das Startups e do Empreendedorismo Inovador, onde foi normatizado o conceito de Sandbox Regulatório (ambiente regulatório experimental), através do inciso II do art. 2º²⁸⁰ no ordenamento jurídico brasileiro (BRASIL, 2021),

279 “A primeira estrutura similar a um sandbox foi estabelecida pelo U.S. Consumer Financial Protection Bureau (CFPB) em 2012 sob o nome de Project Catalyst (CFPB 2016). Em 2015, a Financial Conduct Authority (FCA) do Reino Unido cunhou o termo “sandbox regulatório” (FCA 2015). Desde então, o conceito se espalhou por mais de 20 países, de Abu Dhabi a Serra Leoa.” Tradução do Autor. JENIK, Ivo; LAUER, Kate. Regulatory Sandboxes and Financial Inclusion. CGAP Working Paper. Washington: CGAP, 2017, p. 1

280 BRASIL. Lei Complementar Federal nº. 182, de 1º de junho de 2021. II - ambiente regulatório experimental (sandbox regulatório): conjunto de condições especiais

várias entidades públicas, como autarquias, agências reguladoras, Estados-membros e Municípios vêm implementando diversos modelos de sandboxes regulatórios para solucionar problemas específicos de suas áreas de atuação.

E, naturalmente, diante dessa explosão legislativa e regulamentadora no âmbito das unidades subnacionais, há também a natural preocupação de como serão tratados os dados pessoais obtidos através desses ambientes experimentais.

Anteriormente à instituição e regulamentação dos ambientes regulatórios experimentais, houve a edição e publicação da Lei Geral de Proteção de Dados Pessoais (“LGPD”), Lei Federal nº. 13.709 de 14 de agosto de 2018. Gestada desde 2011, a partir do Anteprojeto de Lei de Proteção de Dados do mesmo ano, o texto foi amplamente debatido com a sociedade civil, através de consultas públicas, resultando em diversas modificações do seu texto original até a consolidação em 2015, possuindo clara inspiração do *General Data Protection Regulation* – GDPR da União Europeia (LIMA, 2018).

A LGPD é uma norma legal bastante didática, apresentando conceitos e princípios que devem ser observados no tratamento de dados pessoais pelos setores da sociedade civil, além de instituir seu próprio órgão regulador, a Autoridade Nacional de Proteção de Dados (“ANPD”), procedimentos de fiscalização e sanções pelos descumprimentos de suas normas; essa última parte entrou em vigor apenas em 2021 (BRASIL, 2018).

E, de forma mais específica, a LGPD dedicou um capítulo exclusivo para o tratamento de dados pessoais pelo setor público, diante da sensibilidade dos dados pessoais por ele coletados, o que impõe o dever de cuidado à Administração Pública na utilização e armazenamento dessas informações. Contudo, esse capítulo não

simplificadas para que as pessoas jurídicas participantes possam receber autorização temporária dos órgãos ou das entidades com competência de regulamentação setorial para desenvolver modelos de negócios inovadores e testar técnicas e tecnologias experimentais, mediante o cumprimento de critérios e de limites previamente estabelecidos pelo órgão ou entidade reguladora e por meio de procedimento facilitado.

abordou de forma mais detalhada como se dá a responsabilidade civil da Administração Pública em casos de violação às regras da LGPD (apenas dois artigos), deixando à cargo da ANPD a criação de padrões e de boas práticas²⁸¹, o que teve início através da Nota Técnica nº 29/2021/CGN/ANPD que criou o Guia Orientativo sobre Tratamento de Dados Pessoais pelo Poder Público, e tampouco abordou como deve ser realizado o tratamento de dados pessoais em ambientes regulatórios experimentais, deixando um vácuo legislativo sobre esse tema.

Este trabalho argumenta que, embora o *sandbox* regulatório seja um instrumento essencial para a inovação em cidades inteligentes, sua aplicação em áreas de alto risco, como a segurança pública, expõe uma perigosa lacuna na proteção de dados pessoais. A ausência de um regime jurídico específico, somada à exceção da LGPD para segurança pública, cria um ambiente de anomia que demanda salvaguardas proativas por parte do regulador, como será demonstrado através da análise do projeto LidEye em Recife.

O primeiro capítulo apresentará o conceito jurídico de ambiente regulatório experimental inaugurado na Declaração Direitos de Liberdade Econômica e, posteriormente, regulamentado pelo Marco Legal das Startups e do Empreendedorismo Inovador e o contexto de criação desse instrumento, inicialmente nos serviços financeiros na Europa e nos Estados Unidos e depois introduzido na jurisdição brasileira. Também será apresentado o conceito de cidades inteligentes e como o uso do *sandbox* regulatório pode auxiliar na consecução dos seus objetivos, como a inclusão digital e redução das desigualdades.

O segundo capítulo apresentará o tratamento da responsabilidade civil da Administração Pública no âmbito da LGPD, introduzindo o próprio conceito de responsabilidade civil do Estado. Em seguida será analisado como é realizado tratamento de dados em ambientes regulatórios experimentais (*sandboxes* regulatórios), abordando especificamente os projetos voltados para segurança pública,

281 Art. 32. A autoridade nacional poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público.

especificamente o Projeto de vídeo vigilância inteligente “LidEye” do segundo ciclo de soluções implantadas em 2024 no Município do Recife e quais medidas e salvaguardas podem ser previstas para regulamentar o tratamento dos dados pessoais coletados na implantação de soluções inovadoras diante da ausência de previsão desse tratamento na LGPD. E, por fim, serão apresentadas ponderações sobre o tratamento de dados em *sandboxes* regulatórios.

Para compreender a profundidade dos desafios que a proteção de dados enfrenta nesses ambientes, é imperativo, primeiramente, dissecar a natureza jurídica e os objetivos do próprio sandbox regulatório. O Capítulo 1, portanto, dedicar-se-á a construir essa base conceitual, explorando o papel do Estado Regulador e o modo como este instrumento catalisa a inovação, especialmente no contexto das cidades inteligentes, preparando o terreno para a análise crítica que se seguirá.

1. SANDBOX REGULATÓRIO.

1.1. O Estado regulador e o Ambiente Regulatório Experimental.

Nas últimas três décadas, a sociedade global vem observando uma explosão de novas tecnologias, observando em quase tempo real a aplicação da Lei de Moore. Essa explosão tecnológica tem sido identificada como Quarta Revolução Industrial, diante da evolução em ritmo exponencial e não linear – com amplitude e profundidade – que provoca mudanças de paradigmas sem precedentes na economia, nos negócios, na sociedade e nos indivíduos; e o impacto sistêmico resultando em transformação de relações entre países e dentro deles, bem como em suas sociedades (SHWAB, 2016).

Diante da magnitude das mudanças desses paradigmas que afetam o componente mais básico de uma sociedade, o próprio indivíduo, ao modificar o seu comportamento social e o seu consumo,

a cidade, membro subnacional mais elementar, não poderia passar ilesa por esta revolução.

Pois, embora a revolução tecnológica proporcione acesso a instrumentos inovadores e oportunidade de novos negócios, é dever das cidades inteligentes promover o acesso equitativo e universal às tecnologias para promover uma maior interação entre o domínio digital e infraestrutura urbana. E para isso, o Ambiente Regulatório Experimental (sandbox regulatório) é o instrumento ideal para atingir esses objetivos.

Isso porque, a Quarta Revolução Industrial impõe desafios regulatórios aos agentes públicos e atores privados de criar um ambiente dedicado para experimentar novos serviços ou produtos, que possibilitam ao agente econômico testar um produto mínimo viável (MVP – minimum viable product) antes de lançá-lo no mercado, bem como oportunizar aos agentes públicos que verifiquem e equalizem quais obrigações regulatórias são adequadas e quais são obsoletas para aquela atividade.

Para isso, foi necessário adequar o modelo jurídico regulatório atual para enfrentar os desafios da inovação tecnológica. Isso porque, o modelo de Estado Regulador, acolhido pela Constituição Federal em seu artigo 174²⁸², estabelece o papel do Estado brasileiro como gestor da atividade econômica nacional, criando as regras jurídicas sobre a regulação econômica, realizando, basicamente, três tipos de atividade: (i) fiscalização, (ii) incentivo e (iii) planejamento. (CARVALHO FILHO, 2009).

Nesse sentido, os *sandboxes* regulatórios são ferramentas ideais para que o Estado moderno possa se preparar para receber e incentivar a produção e criação de novas tecnologias, pois possibilitam a fiscalização do novo produto ou serviço a ser ofertado sem oferecer grandes riscos à população; incentiva através de benefícios e incentivos

282 BRASIL. **Constituição Federal de 5 de outubro de 1988**. Art. 174. Como agente normativo e regulador da atividade econômica, o Estado exercerá, na forma da lei, as funções de fiscalização, incentivo e planejamento, sendo este determinante para o setor público e indicativo para o setor privado.

fiscais e relaxamento de salvaguardas e obrigações; e estabelece metas e objetivos para o fortalecimento econômico e tecnológico.

E são, igualmente, instrumentos de ruptura do ponto de vista teórico do conceito tradicional de Estado Regulador. Feigelson e Leite (2020) entendem que esse fato, por si só, constitui grande ruptura com a percepção tradicional de tal contexto, visto que a inovação, por essência, é um processo de tentativa, erro e aprendizado, e, tradicionalmente, a sociedade não aceita erros. Do ponto de vista normativo, supor que o regulador possa se dar ao luxo de “experimental” a melhor forma de regular determinado tema é uma quebra de paradigma.

Como brevemente exposto na Introdução, os *sandboxes* regulatórios foram inicialmente utilizados no setor financeiro dos Estados Unidos e do Reino Unido e hoje, de acordo com o Banco Mundial²⁸³, em 2020, mais de 57 jurisdições fazem uso desse expediente, demonstrando a disseminação desta ferramenta por países em todas as regiões do globo.

Da mesma forma no Brasil, o setor financeiro foi quem iniciou o uso dos ambientes regulatórios experimentais através do Banco Central do Brasil²⁸⁴, seguido pelo setor de seguros através da Superintendência de Seguros Privados (Susep)²⁸⁵ e o mercado de capitais, através da Comissão de Valores Mobiliários (CVM)²⁸⁶.

283 World Bank, 2020. **Key Data from Regulatory Sandboxes across the Globe.** Disponível em <https://www.worldbank.org/en/topic/fintech/brief/key-data-from-regulatory-sandboxes-across-the-globe>. Acesso em 16 de julho de 2024.

284 BRASIL. Banco Central do Brasil. Resolução no 50, de 16 de dezembro de 2020. **Dispõe sobre os requisitos para instauração e execução pelo Banco Central do Brasil do Ambiente Controlado de Testes para Inovações Financeiras e de Pagamento (Sandbox Regulatório) – Ciclo 1, bem como sobre os procedimentos e requisitos aplicáveis à classificação e à autorização para participação nesse ambiente.** Brasília: Banco Central do Brasil, 17 dez. 2020. Disponível em: <https://www.bcb.gov.br/estabilidade/financeira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=50>. Acesso em 16 de julho de 2024.

285 SUSEP, 2019. **Implantação de regime de sandbox regulatório nos mercados financeiros e de capitais brasileiro.** Disponível em <https://www.gov.br/susep/pt-br/central-de-conteudos/noticias/2022/noticia> Acesso em 16 de julho de 2024.

286 BRASIL. Comissão de Valores Mobiliários. Resolução CVM no 29, de 11 de maio de 2021. **Dispõe sobre as regras para constituição e funcionamento de ambiente regulatório experimental (sandbox regulatório) e revoga a Instrução CVM no 626,**

Rapidamente esse modelo de regulação se espalhou pelo país, saindo da esfera federal para ser adotado pelos Municípios, tais como Rio de Janeiro²⁸⁷, João Pessoa²⁸⁸, Recife²⁸⁹, dentre outros.

Em todos os casos analisados, o sandbox regulatório tem como objetivo fomentar a inovação tecnológica da área de atuação do órgão regulador (nos casos das autarquias e agências reguladoras) ou fomentar o desenvolvimento econômico e tecnológico no âmbito local, com o objetivo de atrair investimentos e estimular a criação de novos negócios, melhorar a eficiência dos serviços públicos oferecidos à população e fortalecer a ciência de base.

E para que esses ambientes especiais tenham êxito nos objetivos propostos em suas normas instituidoras, segundo Quirino, Hocayean e Cunha (2023, p. 15), eles devem possuir quatro características essenciais, quais sejam: (i) o afastamento das regras e normas aplicáveis para a testagem de determinado produto ou serviço; (ii) a delimitação do escopo da testagem; (iii) a delimitação temporal da testagem; e (iv) a observação e avaliação constante dos resultados.

Em outras palavras, é necessário que seja criado um suporte normativo que conceda um relaxamento ou completo afastamento de determinadas regras restritivas, estabeleça a delimitação geográfica, definição dos requisitos de acesso às entidades participantes, objeto, limite temporal para implementação e funcionamento do projeto e o público-alvo.

de 15 de maio de 2020. Disponível em <https://conteudo.cvm.gov.br/export/sites/cvm/legislacao/resolucoes/anexos/001/resol029.pdf>. Acesso em 16 de julho de 2024.

287 RIO DE JANEIRO. **Decreto Municipal nº. 50.697 de 26 de abril de 2022.** Disponível em [https://doweb.rio.rj.gov.br/apifront/portal/edicoes/imprimir_materia/825386/5322#:~:text=ABRIL%20DE%202022-,Disp%C3%B5e%20sobre%20as%20regras%20para%20cria%C3%A7%C3%A3o%20e%20funcionamento%20de%20ambiente,regulat%C3%B3rio\)%2C%20e%20outras%20provid%C3%AAs](https://doweb.rio.rj.gov.br/apifront/portal/edicoes/imprimir_materia/825386/5322#:~:text=ABRIL%20DE%202022-,Disp%C3%B5e%20sobre%20as%20regras%20para%20cria%C3%A7%C3%A3o%20e%20funcionamento%20de%20ambiente,regulat%C3%B3rio)%2C%20e%20outras%20provid%C3%AAs). Acesso em 16 de julho de 2024.

288 JOÃO PESSOA. **Lei Municipal nº. 14.092 de 30 de dezembro de 2020.** Disponível em <https://leismunicipais.com.br/a/pb/j/joao-pessoa/lei-ordinaria/2020/1410/14092/lei-ordinaria-n-14092-2020-dispoe-sobre-as-regras-para-constituicao-e-funcionamento-de-ambiente-regulatorio-experimental-sandbox-regulatorio-no-municipio-de-joao-pessoa>. Acesso em 16 de julho de 2024.

289 RECIFE. **Decreto Municipal nº. 35.511 de 01 de abril de 2022.** Disponível em <http://leismunicipa.is/zdwua>. Acesso em 28 de maio de 2024.

É importante destacar que esse suporte normativo não precisa ser uma lei em sentido estrito, isto é, uma norma legal aprovada pelo Parlamento (nacional, estadual ou municipal) para que o Poder Executivo possa instituir um sandbox regulatório.

Isso porque, o Marco Legal das Startups e do Empreendedorismo Inovador e a Declaração Direitos de Liberdade Econômica são leis de caráter nacional diante da sua transcendência reguladora de questões de política interna dos entes que compõem a Federação, atingindo e estabelecendo critérios uniformizadores em todo País.

Portanto, essas normas legais estabelecem como direito dos cidadãos e das empresas brasileiras ter um ambiente favorável para o desenvolvimento econômico através do empreendedorismo inovador, com o objetivo de desburocratizar e simplificar a atividade empresarial diante do reconhecimento que a legislação não consegue acompanhar o desenvolvimento tecnológico. Nesse contexto, o excesso e engessamento burocrático e regulatório pode impedir esse desenvolvimento, tornando o microssistema do ambiente regulatório experimental o meio ideal para atingir esse objetivo.

1.2 Ambiente Regulatório Experimental como instrumento catalisador para criação de novas tecnologias em Cidades Inteligentes.

O uso pioneiro de *sandboxes* regulatórios por agências reguladoras, em especial, pelo setor financeiro, decorre da necessidade das empresas desse setor econômico precisarem atualizar de forma perene os seus sistemas para evitar ataques de pessoas e entidades mal-intencionadas e evitar a prática de atividades criminosas no sistema financeiro.

O êxito dessa prática no sistema bancário resultou na replicação do modelo nos demais setores econômicos, sempre sob o guarda-chuva das entidades reguladoras. Naturalmente, o sucesso comprovado de uma ferramenta resulta na popularização do seu uso, exatamente o que ocorreu com os ambientes regulatórios experimentais diante

do acolhimento pelas demais entidades públicas da Federação, em especial, os Municípios.

O uso dos *sandboxes* regulatórios pelos Municípios é especialmente importante diante do crescimento das cidades, onde hoje mais pessoas habitam centros urbanos do que zonas rurais²⁹⁰, aliado ao aumento da conectividade frente a multiplicação de aparelhos com acesso à internet e à luz do surgimento de novas tecnologias em espaços de tempo cada vez mais curtos, é natural que os gestores municipais busquem formas inovadoras de prestar serviços públicos para o atendimento do interesse da coletividade.

Essa procura em buscar as melhores soluções para o uso inteligente da tecnologia no planejamento urbano e na melhoria da infraestrutura local tem sido objeto de interesse de diversos gestores públicos desde a década de 1990, quando surgiu o conceito *smart cities* (cidades inteligentes), que logo foi estudado pelos Estados e por organizações supranacionais.

A OCDE entende que o conceito de cidade inteligente varia de acordo com cada País, mas em termos gerais, define como iniciativas ou abordagens que utilizam de forma eficaz a digitalização para aumentar o bem-estar dos cidadãos e proporcionar serviços urbanos e ambientes mais eficientes, sustentáveis e inclusivos, como parte de um processo colaborativo e com múltiplas partes interessadas (OCDE, 2020)²⁹¹.

Atenta a essas movimentações o Governo Federal publicou em 2021 a chamada Carta Brasileira para as Cidades Inteligentes. Essa carta se originou de uma iniciativa do Ministério de Desenvolvimento Regional (MDR), hoje, Ministério das Cidades, com o apoio da Agência de Cooperação Alemã GIZ e em parceria com o Ministério de Ciência,

290 Segundo o Relatório Mundial das Cidades, publicado pelo ONU-Habitat em 2022, as áreas urbanas já abrigam 55% da população global, devendo chegar a 68% até 2050. Esse número sobe para 81% ao se considerar a região da América Latina e do Caribe, e segundo o IBGE, chega a 85% quando o foco é o Brasil. Disponível em <https://brasil.un.org/pt-br/240326-relat%C3%B3rio-anual-do-onu-habitat-tem-experi%C3%Aancia-interativa#:~:text=Segundo%20o%20Relat%C3%B3rio%20Mundial%20das,o%20foco%20C3%A9%20o%20Brasil>. Acesso em 28 de julho de 2024.

291 Tradução do Autor.

Tecnologia e Inovações (MCTI), com o Ministério das Comunicações (MCom) e várias organizações privadas e apresenta a seguinte definição:

Aquele documento define como cidade inteligente aquelas comprometidas com o desenvolvimento urbano e a transformação digital sustentáveis, em seus aspectos econômico, ambiental e sociocultural, que atuam de forma planejada, inovadora, inclusiva e em rede, promovem o letramento digital, a governança e a gestão colaborativas e utilizam tecnologias para solucionar problemas concretos, criar oportunidades, oferecer serviços com eficiência, reduzir desigualdades, aumentar a resiliência e melhorar a qualidade de vida de todas as pessoas, garantindo o uso seguro e responsável de dados e das tecnologias da informação e comunicação.

Essa Carta tem como justificativa a redução da desigualdade social através da transformação e inclusão digital e uso de novas tecnologias para transformar a infraestrutura digital em infraestrutura urbana (BRASIL, 2021).

Além dessas definições, há propostas legislativas que tentam instituir políticas públicas para cidades inteligentes, como o Projeto de Lei nº. 976/2021 que almeja criar a Política Nacional de Cidades Inteligentes – PNCI. Ele tenta normatizar o conceito de cidade inteligente como “espaço urbano orientado para o investimento em capital humano e social, o desenvolvimento econômico sustentável e o uso de tecnologias disponíveis para aprimorar e interconectar os serviços e a infraestrutura das cidades, de modo inclusivo, participativo, transparente e inovador, com foco na elevação da qualidade de vida e do bem-estar dos cidadãos” (BRASIL, 2021).

A literatura jurídica também já tratou sobre esse instituto. Andrade (2023, p.109) entende que esse conceito ignora os comandos constitucionais das funções sociais da cidade e que vinculam toda e qualquer política sobre o desenvolvimento das cidades brasileiras, mas esse conceito, em sua visão, centraliza os serviços públicos e a infraestrutura como objeto material da PNCI, visando a qualidade de vida e o bem-estar dos cidadãos, que deve ser obtido por ferramentas

efetivas que proporcionem e criem condições de realização dos direitos fundamentais.

Além da tentativa de conceituação jurídica, há outras entidades que apresentam conceitos mais técnicos sobre as cidades inteligentes. A ABNT publicou em abril de 2019 a “NORMA ABNT NBR ISSO 37122:2020 Cidades e comunidades sustentáveis – indicadores para cidades inteligentes”. Essa norma é a internalização do ISSO 37122 de maio de 2019. Esse regulamento normatiza, no item 3.4, a cidade inteligente como uma cidade que aumenta o ritmo em que proporciona resultados de sustentabilidade social, econômica e ambiental e que responde a desafios como mudanças climáticas, rápido crescimento populacional e instabilidades de ordem política e econômica, melhorando fundamentalmente a forma como engaja a sociedade, aplica métodos de liderança colaborativa, trabalha por meio de disciplinas e sistemas municipais, e usa informações de dados e tecnologias modernas, para fornecer melhores serviços e qualidade de vida para os que nela habitam (residentes, empresas, visitantes), agora e no futuro previsível, sem desvantagens injustas ou degradação do ambiente natural (2020, p.18).

Sobre essa norma, Andrade (2023) acredita que ela procura estabelecer critérios internacionalmente definidos para avaliar se, como, e em qual medida as cidades brasileiras têm incorporado as noções globalmente difundidas sobre cidades inteligentes.

Mas essa avaliação é realizada sob premissas estabelecidas internacionalmente através de experiências de cidades que vivem uma realidade discrepante da realidade da absoluta maioria das cidades brasileiras.

Por isso é necessário adequar essas experiências à realidade local para que se possa obter resultados que atendam aos anseios dessas comunidades do que implementar projetos pensados em padrões muito distantes daqueles que vivem o cidadão médio brasileiro. Isto é, utilizar as novas tecnologias para melhorar a qualidade dos serviços públicos e privados sob a ótica da realidade brasileira.

Assim, com o rápido e fácil acesso a essas novas ferramentas, novos horizontes se desdobram para auxiliar na melhoria do planejamento urbano, instando gestores públicos a promover a inclusão dessas ferramentas no dia a dia das pessoas em favor das comunidades, trazendo para o cidadão os avanços e benefícios da Quarta Revolução Industrial.

Há diversos exemplos do uso dessas tecnologias pelas cidades. Antonialli e Kira (2020) apresentam como a Prefeitura de Chicago desenvolveu um algoritmo para otimizar as inspeções sanitárias dos restaurantes da cidade, como a Prefeitura do Distrito de Columbia criou um canal para que os munícipes possam avaliar os serviços públicos prestados pela capital americana ou ainda como a cidade de Nova Iorque criou um projeto em que é disponibilizada a identificação de terrenos públicos para que a população possam observar o tratamento dado pelo Poder Público no cuidado com a coisa pública.

Assim, é possível utilizar o Ambiente Regulatório Experimental para implementar diversas soluções de interesse público de forma controlada e, após testada a sua eficiência, possa ser oferecida à população, transformando as cidades brasileiras em cidades inteligentes.

O sucesso do sandbox regulatório como catalisador de cidades inteligentes, exemplificado por iniciativas como o ‘Recife Living Labs’, cria, contudo, uma série de complexidades jurídicas. Ao flexibilizar normas para testar tecnologias inovadoras, muitas das quais, por sua natureza, dependem da coleta e tratamento massivo de dados pessoais, este ambiente experimental cria uma tensão direta com os princípios e regras estabelecidos pela Lei Geral de Proteção de Dados. É precisamente nesta intersecção entre a inovação desregulamentada e o direito fundamental à privacidade que reside o núcleo deste trabalho. Tendo estabelecido o que é e para que serve o sandbox, o próximo capítulo se aprofundará nas consequências dessa tensão, analisando a responsabilidade da Administração Pública e os riscos inerentes ao tratamento de dados em um ambiente concebido para a exceção.

2. TRATAMENTO DE DADOS NO SANDBOX REGULATÓRIO.

2.1. Responsabilidade e deveres da Administração Pública no âmbito do tratamento de dados pessoais.

A responsabilidade é um instituto amplamente tratado pelo Direito nacional, sendo objeto de estudo de quase todas as áreas jurídicas, desde penal até tributária. De forma mais básica, a ideia de responsabilidade advém de resposta, isto é, a responsabilidade implica em impor a alguém o dever de responder sobre algum ato ou fato.

Dessa ideia nasce o conceito de fato e imputabilidade, que são dois pressupostos inafastáveis para fins de caracterização de qualquer responsabilidade. Quer dizer, é preciso a ocorrência de um fato, omissivo ou comissivo, e a existência de alguém com capacidade jurídica para responder por esse fato para que a responsabilidade possa ser imposta (CARVALHO FILHO, 2009).

No âmbito das relações privadas, a responsabilidade civil foi inicialmente fundamentada no conceito de culpa, no ato ilícito indenizável. Porém somente esse alicerce foi considerado insuficiente, já que a ideia de reparação é muito mais ampla do que a do ato ilícito, pois há casos passíveis de indenização em que não se cogita a ilicitude da conduta do agente. E, já há algum tempo, o ordenamento jurídico caminha para inversão do fundamento da responsabilidade civil. Se a regra antes era a responsabilidade com culpa, hoje é possível afirmar que esta é exceção e a regra é a responsabilidade sem culpa (PEREIRA, 2014).

É o que se observa com o Código de Defesa do Consumidor que abraçou a teoria da responsabilidade objetiva; o Decreto Federal nº. 7.962/2013, que regulamenta o comércio eletrônico, atribuindo a responsabilidade civil objetiva também para essa modalidade negocial, e posteriormente a própria LGPD ao estabelecer a responsabilidade objetiva do controlador de dados (art. 43).

Nas relações jurídicas de direito público, o conceito de responsabilidade objetiva há muito está positivado na Constituição

Federal (§6º do art. 37) ao dispor que as pessoas jurídicas de direito público e as de direito privado prestadoras de serviços públicos responderão pelos danos que seus agentes, nessa qualidade, causarem a terceiros, assegurado o direito de regresso contra o responsável nos casos de dolo ou culpa (BRASIL, 1988).

Essa previsão constitucional, ratificada na LGPD, advém da característica da relação jurídica estabelecida entre o Poder Público e o indivíduo titular de dados pessoais, que é marcada pela assimetria de poder, decorrente de duas premissas: o poder de império que detém o Estado em suas relações e a posse de grande quantidade de dados pessoais em seus bancos de dados, um subproduto oriundo do desempenho de sua atividade (TASSO, 2021).

Dessa forma, ao reconhecer a disparidade de poder nessas relações, a LGPD apresentou tratamento específico, como exposto no capítulo introdutório, no tratamento de dados pessoais pelo Poder Público diante do uso massivo de dados dos cidadãos pelos órgãos públicos para fins de implementação de políticas públicas, tais como serviços de saúde.

A lei de proteção de dados impôs aos gestores públicos o dever de transparência no tratamento dos dados pessoais, elencando as hipóteses legais em que o Poder Público poderá realizar o tratamento desses dados, sempre com o objetivo de atender a finalidade e o interesse público. Trata-se, portanto, de uma atuação condicionada, isto é, uma atuação sempre motivada e que dever atender a uma política pública pré-estabelecida sem qualquer caráter discricionário.

Quando o art. 23 da LGPD estabelece que as pessoas públicas indicadas no art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação)²⁹² são as mesmas submetidas a sua fiscalização

292 Art. 1º Esta Lei dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal. Parágrafo único. Subordinam-se ao regime desta Lei: I - os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público; II - as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia

expõe o caráter de transparência que o legislador ordinário quis dar à norma legal.

Nesse sentido, a ANPD apresenta o primeiro esforço em regulamentar e delimitar as interpretações da LGPD para a Administração Pública, através da Nota Técnica nº 29/2021/CGN/ANPD que criou o Guia Orientativo sobre Tratamento de Dados Pessoais pelo Poder Público²⁹³. Neste guia, a Autoridade Nacional apresenta orientações sobre as bases legais e os princípios que devem nortear o tratamento de dados pessoais por entidades e órgãos públicos.

Dessa forma, a agência reguladora aponta que a administração pública deve observar princípios da segurança, da prevenção e da responsabilização e prestação de contas, adotando medidas técnicas e administrativas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais. Esse imperativo tem aplicação ampla, pois devem segui-lo todos os órgãos e entidades dos entes federativos, dos três Poderes, órgãos de fiscalização de contas públicas, Ministérios Públicos, serviços notariais e as empresas públicas e as sociedades de economia mista desde que não estejam atuando em regime de concorrência; ou operacionalizem políticas públicas, no âmbito da execução destas²⁹⁴.

A falha no cumprimento desses deveres gera a responsabilização do ente ou órgão da administração pública, através de sanções não-pecuniárias previstas na LGPD, tais como advertência, publicização da infração pelo órgão público infrator, bloqueio dos dados pessoais até a regularização da infração cometida, suspensão do exercício da atividade de tratamento de dados, proibição total ou parcial do

mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios.

293 ANPD, **Guia Orientativo sobre Proteção de Dados Pessoais pelo Poder Público**. Disponível em <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf>. Acesso em 30 de dezembro de 2024.

294 Artigos 46 a 49 da LGPD.

exercício de atividades relacionados a tratamento de dados, entre outros.²⁹⁵

Com relação à multa pecuniária, não há vedação expressa na legislação que afaste a possibilidade de aplicação da sanção em face de órgãos públicos diante do texto do §3º do art. 52. Contudo, ao analisar o parecer do Deputado Federal Orlando Silva, relator da Comissão Especial, a *mens legis* aponta para a vedação dessa penalidade, ao dispor que seria apropriada a aplicação das sanções de advertência, publicização da infração, bloqueio e eliminação de dados pessoais, suspensão parcial ou total de funcionamento de banco de dados, suspensão do exercício de atividade de tratamento e a proibição parcial ou total do exercício dessas atividades (BRASIL, 2012)²⁹⁶.

Por outro lado, há doutrinadores que apontam que a norma legal não vedou expressamente essa possibilidade, haja vista a escolha dos verbos para compor a oração do §3º do art. 52. Isso porque, o verbo “poderá” não possui suficiente semântica de restrição de disposição legal, pelo contrário, expande para compreender permissividade, adição, complementação (ALVES, 2021). Além disso, o afastamento da possibilidade de aplicação multas pecuniárias poderá enfraquecer a cogência da norma, já que o Poder Público é o maior controlador de dados diante da necessidade de obtenção dessas informações para prestação de serviços públicos essenciais, o que parece ser contraproducente com o objetivo da LGPD de impor maiores responsabilidades aos controladores de dados.

De toda sorte, há a possibilidade de responsabilização pessoal do servidor público que infringir a LGPD ao tratar os dados pessoais de forma indevida ou para fins ilícitos, nos termos do disposto na Lei de

295 Art. 52. (...)§ 3º O disposto nos incisos I, IV, V, VI, X, XI e XII do caput deste artigo poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei nº 8.112, de 11 de dezembro de 1990, na Lei nº 8.429, de 2 de junho de 1992, e na Lei nº 12.527, de 18 de novembro de 2011.

296 Câmara dos Deputados, Parecer do Relator, Dep. Orlando Silva. Disponível em https://www.camara.leg.br/proposicoesWeb/prop_m. Acesso em 14 de janeiro de 2025.

Introdução às Normas do Direito Brasileiro²⁹⁷ e no Decreto Federal nº. 10.046/2019²⁹⁸, para os casos de compartilhamento indevido de dados pessoais tratados pela administração pública. Além disso, há ainda que a violação dolosa da LGPD por agente público pode constituir ato de improbidade administrativa, cabendo sua responsabilização pessoal, nos termos do art. 11, IV, da Lei nº. 8.429/1992²⁹⁹, sem prejuízos de aplicação de outras penalidades.

Em 2022, o Supremo Tribunal Federal decidiu, no julgamento conjunto da Ação Direta de Inconstitucionalidade (“ADI”) nº. 6.649 e da Arguição de Descumprimento de Preceito Fundamental (“ADPF”) nº. 695, ao julgar a constitucionalidade do Decreto Federal nº. 10.046/2019, que regulamenta o compartilhamento de dados pessoais, assegurou que os órgãos da Administração Pública devem observar com rigor os preceitos e fundamentos da LGPD, sob pena de imputação de responsabilidade civil do Estado pelos danos suportados pelo titular dos dados, nos termos do art. 42³⁰⁰ e seguintes da lei de proteção de dados, assegurado o direito de regresso contra os servidores e agentes que agirem com culpa ou dolo (BRASIL, 2022).

Assim, mesmo diante do tratamento de dados pelo Poder Público, a LGPD busca zelar pela transparência da atividade estatal, possibilitando ao titular dos dados pessoais o direito ao efetivo controle

297 Decreto-Lei nº. 4.657/1942. Art. 28. O agente público responderá pessoalmente por suas decisões ou opiniões técnicas em caso de dolo ou erro grosseiro.

298 Art. 15-A. O tratamento de dados pessoais, em qualquer nível de categorização para compartilhamento, pelos órgãos e pelas entidades de que trata o art. 1º, está sujeito ao atendimento dos parâmetros legais e constitucionais e importará a responsabilidade civil do Estado pelos danos suportados pelos particulares. (Incluído pelo Decreto nº 11.266, de 2022) Parágrafo único. O disposto no caput está associado ao exercício do direito de regresso contra os agentes públicos responsáveis pelo ato ilícito, em caso de culpa ou dolo. (Incluído pelo Decreto nº 11.266, de 2022)

299 Art. 11. Constitui ato de improbidade administrativa que atenta contra os princípios da administração pública a ação ou omissão dolosa que viole os deveres de honestidade, de imparcialidade e de legalidade, caracterizada por uma das seguintes condutas:

300 Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

sobre os seus dados, especialmente diante da elevação da proteção dos dados pessoais como direito fundamental após a promulgação da Emenda Constitucional nº. 115 que incluiu o inciso LXXIX ao rol do art. 5º da Constituição Federal, constituindo-se como cláusula pétrea³⁰¹, bem como a possibilidade de responsabilização da máquina pública e dos seus gestores pelo uso indevido dos dados pessoais.

Se a responsabilidade do Estado já é um tema complexo sob o regime geral da LGPD, ela adquire contornos ainda mais sérios quando o tratamento de dados ocorre em um ambiente duplamente excepcional: um sandbox regulatório cujo objeto é, precisamente, uma das atividades excluídas do escopo da lei; a segurança pública. A capítulo seguinte analisará este cenário de alto risco.

2.2. Uso de dados pessoais em sandboxes regulatórios e em atividades de segurança pública.

Como já apresentado, a LGPD não trouxe tratamento específico para os dados pessoais coletados em ambientes regulatórios experimentais. Aplicando-se, assim, a regra geral de tratamento de dados pelas pessoas jurídicas de direito privado que estejam atuando em *sandboxes* regulatórios e as regras para o Poder Público para os agentes públicos que realizarem o tratamento de dados obtidos nesses ambientes.

Isto é, a LGPD não excepcionou ou flexibilizou o tratamento de dados em ambientes regulatórios experimentais e nem deu tratamento diferenciado para as entidades que estejam participando dos editais lançados pelos órgãos públicos.

Contudo, há esforços para aumentar a regulação do tratamento de dados nos ambientes de Cidades Inteligentes, como o Projeto de Lei nº. 976/2021 que almeja criar a Política Nacional de Cidades Inteligentes – PNCI. Nesse projeto de lei, há a tentativa, ainda tímida, de trazer segurança jurídica ao tratamento de dados pessoais em

301 LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais. (Incluído pela Emenda Constitucional nº 115, de 2022)

soluções criadas para Cidades Inteligentes, como o §2º do art. 5º que estabelece como diretriz a observância da privacidade e da segurança no tratamento de dados pessoais³⁰², levando em consideração a necessária garantia da proteção dos dados pessoais e o uso das melhores práticas (BRASIL, 2021).

Portanto, na ausência de uma regulação específica, deve-se observar a regra geral de tratamento de dados pessoais em ambientes regulatórios experimentais, devendo os órgãos públicos e as entidades participantes dos editais seguir as bases legais para o tratamento dos dados pessoais.

A LGPD estabelece alguns parâmetros imprescindíveis que devem ser observados pelas entidades para que o tratamento de dados possa ser realizado de forma adequada. Assim, a norma aponta que qualquer agente de tratamento deve indicar uma base legal para lastrear o uso dos dados pessoais coletados em sua atividade, devendo realizar a adequação em ao menos uma hipótese legal prevista nos artigos 7º e 11 para que o tratamento possa ser considerado legítimo, possibilitando, inclusive, o acúmulo de bases legais de acordo com o contexto da operação realizada. Isso porque, apesar do rol previstos nestes dispositivos serem taxativos, são dotados de hipóteses mais abertas e com certo grau de subjetividade (chamadas de hipóteses “coringas”), o que facilita a realização do tratamento adequado (TEFFÉ e VIOLA, 2020).

O mesmo tratamento deve ser observado pela Administração Pública.

A administração pública deve justificar como base legal para o tratamento de dados pessoais a execução de política pública, persecução do interesse público ou o cumprimento de atribuições legais do serviço público, de acordo com a determinação do artigo

302 Art. 5º O desenvolvimento de iniciativas de cidades inteligentes deverá observar as seguintes diretrizes: § 2º A observância da privacidade e da segurança de que trata o inciso XIV deverá levar em consideração a necessária garantia da proteção dos dados pessoais e o uso das melhores práticas, em conformidade com a Lei nº 13.709, de 14 de agosto de 2018.

23 da LGPD³⁰³, mediante o cumprimento dos seguintes requisitos: (i) sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos; e (ii) seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais.

Esse artigo 23 traz requisitos adicionais para o tratamento de dados pessoais pela administração pública, partindo da base legal do cumprimento de uma obrigação legal (II, art. 7º; ‘a’, II, art. 11) ou da execução de uma política pública (III, art. 7º; ‘b’, II, art. 11), não constituindo uma base legal em si mesma, pois o tratamento de dados pessoais para essas atividades já estaria contemplado nas disposições do art. 7º e 11 (TEFFÉ e VIOLA, 2020).

Assim, projetos e soluções voltadas para ambientes de Cidades Inteligentes constituem bases legais permitidas pela LGPD para o tratamento de dados pessoais, pois atendem a consecução de políticas públicas, tais como a segurança pública na implantação de infraestrutura inteligente e sistemas de monitoramento, possibilitando as cidades inteligentes melhorar e otimizar os serviços públicos, tais como a segurança pública e a resposta à emergências, através de sensores, câmeras de vigilância e algoritmos avançados, através inclusive do uso de Inteligência Artificial através de modelos de linguagem de grande escala (LLM, no acrônimo em inglês).

Sobre a área de segurança pública, ela compõe, inclusive, um dos 17 Objetivos de Desenvolvimento Sustentável (ODS) da Agenda 2030 da Organização das Nações Unidas (ONU)³⁰⁴. O ODS 16 possui

303 Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:

304 ONU, Agenda 2030 para o Desenvolvimento Sustentável. Disponível em <https://brasil.un.org/pt-br/91863-agenda-2030-para-o-desenvolvimento-sustent%C3%A1vel>. Acesso em 14 de janeiro de 2025.

como premissa a promoção de sociedades pacíficas e inclusivas para o desenvolvimento sustentável e proporcionar o acesso à justiça para todos e construir instituições eficazes, responsáveis e inclusivas em todos os níveis, mediante a redução de todas as formas de violência e as taxas de mortalidade relacionada em todos os lugares. Com base nesse objetivo, observa-se que alguns entes federativos têm recebidos propostas de projetos e soluções voltadas para essa área, como no caso do Programa “Recife Living Labs”, também conhecido como EITA Labs³⁰⁵, *sandbox* regulatório instituído pelo Município do Recife através do Decreto Municipal nº. 35.511 de 01 de abril de 2022.

No segundo ciclo de soluções implantadas em 2024, há o projeto “LidEye” da empresa Grupo Liderança com o prazo de 12 (doze) meses de experimentação. Esse projeto possui como objetivo a implantação de uma rede colaborativa de vídeo vigilância inteligente através de algoritmos de inteligência artificial e integração do sistema ao Centro de Controle Operacional local para o monitoramento preventivo e repressivo para o fim da redução dos índices criminais.³⁰⁶

Contudo, o uso de dados pessoais para segurança pública possui regramento diferenciado pela LGPD.

Isso porque, uso desses dados passa quase sempre pelo tratamento disposto no art. 11, isto é, tratamento de dados sensíveis. A LGPD conceitua dados sensíveis como dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural³⁰⁷.

Assim, necessariamente o tratamento de dados pessoais para a segurança pública, em especial projetos e soluções que utilizem a imagem das pessoas, perpassará pelo tratamento de dados sensíveis,

305 <https://sites.google.com/recife.pe.gov.br/eitalabs/>. Acesso em 14 de janeiro de 2025.

306 <https://sites.google.com/recife.pe.gov.br/eitalabs/solu%C3%A7%C3%B5es-implantadas/2%C2%BA-ciclo-2024/lideye>. Acesso em 14 de janeiro de 2025.

307 Art. 5º, II da LGPD.

em especial dados que forneçam informações sobre a origem racial ou ética do indivíduo ou informações biométricas, mediante a captura através de câmeras de vigilância.

Todavia, o uso de dados pessoais para essa atividade constitui uma exceção à proteção dada pela LGPD, inclusive o tratamento de dados sensíveis. O art. 4º excetua os casos em que a lei de proteção de dados não é aplicável, dentre eles, para segurança pública³⁰⁸. E essa exceção também engloba as pessoas jurídicas de direito privado que estiverem atuando sob a tutela de pessoa jurídica de direito público, mediante envio de relatórios específicos para a ANPD³⁰⁹.

Essa exceção não é exclusiva da lei nacional, pois a GDPR igualmente excepcionou a sua aplicação para o tratamento de dados pessoais realizados pelas autoridades competentes para as atividades de investigação, prevenção de infrações penais e para execução de sanções penais³¹⁰.

É necessária a existência de regulação do tratamento de dados nessa área, especialmente diante do uso de *sandboxes* regulatórios para teste e implementação de projetos nesta seara. Nesse sentido, há em tramitação na Câmara dos Deputados o Projeto de Lei nº. 1.515 de 2022, o chamado “LGPD Penal”, que visa regulamentar o tratamento de dados nas áreas de segurança pública e defesa nacional³¹¹, além do Anteprojeto de Lei de Proteção de Dados Pessoais para Segurança Pública e Persecução Penal elaborado por uma comissão de juristas para a Presidência da Câmara dos Deputados.

308 Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais: III - realizado para fins exclusivos de: a) segurança pública;

309 Art. 4º. (...), III – (...) § 2º É vedado o tratamento dos dados a que se refere o inciso III do caput deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo.

310 Art. 2º, item 2, d do GDPR.

311 Disponível em https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2182274&filename=PL%201515/2022. Acesso em 15 de janeiro de 2025.

A análise do projeto LidEye, operando na interseção de um ambiente experimental com a lacuna regulatória da segurança pública, demonstra a magnitude do risco aos direitos fundamentais. A ausência de uma LGPD Penal e de regras específicas para o tratamento de dados em sandboxes cria uma zona cinzenta que não pode ser ignorada. Diante deste vácuo legislativo cabe, portanto, ao próprio regulador, na estruturação do edital e dos termos de autorização do sandbox, construir as salvaguardas que a lei não previu. A seção a seguir explorará quais medidas protetivas concretas podem e devem ser implementadas para mitigar esses riscos.

2.3. Possíveis medidas de proteção e salvaguardas pelo regulador.

Diante dessa lacuna legislativa, é necessário que os reguladores estabeleçam critérios e medidas de salvaguardas no documento-base que instituir os *sandboxes* regulatórios, de forma genérica, que possam ser impostas aos participantes do programa para o tratamento de dados pessoais, atendendo o dever de *compliance* necessário, especialmente diante de projetos voltados para a segurança pública.

Um bom exemplo são as diretrizes gerais estabelecidas pelo Laboratório de Inovação Financeira (“LAB”)³¹² para instituição de *sandboxes* regulatórios no âmbito do mercado financeiro brasileiro, setor que também coleta dados sensíveis e sigilosos, cujas sugestões podem ser aplicadas para soluções e projetos de outros mercados econômicos.

O LAB apresenta um rol de salvaguardas que podem ser aplicadas pelo Comitê Gestor do *sandbox*, observando as características e especificidades de cada eixo temático ou área de interesse econômico:

312 O Laboratório de Inovação Financeira (LAB) é um projeto conjunto da Associação Brasileira de Desenvolvimento (ABDE), do Banco Interamericano de Desenvolvimento (BID) e da Comissão de Valores Mobiliários (CVM), lançado em agosto de 2017, que funciona como um fórum de discussão multissetorial, para a promoção das finanças sustentáveis e da inovação financeira no país. Disponível em <http://labinovacaofinanceira.com/quem-somos/>. Acesso em 15 de janeiro de 2025.

(i) limitação quanto ao número de clientes e usuários que as empresas participantes poderão acessar durante o período de testes e a sua a qualificação mínima; (ii) limitação quanto ao volume máximo de recursos que pode ser operado pelas empresas participantes; (iii) formas de divulgação aos clientes e usuários a respeito dos riscos associados à empresa participante do programa de *sandbox*; e (iv) exigência de mecanismos para sua cobertura ou indenização por prejuízos incorridos pelos usuários³¹³ (LAB, 2019).

A previsão da salvaguarda do item (iii) é de extrema importância, especialmente quando observamos o princípio da transparência³¹⁴ e a necessidade de consentimento do titular de dados pessoais para que o tratamento dos seus dados seja realizado, como fundamento à autodeterminação informativa³¹⁵ e a ausência de regramento específico sobre o tratamento de dados em *sandboxes* regulatórios, conforme já abordado no capítulo anterior.

Assim, estaria preservando o chamado consentimento contextual em que o cidadão permanece exercendo o domínio sobre os seus dados, ainda que sem declarar expressamente a sua vontade diante do tratamento previsível dos seus dados em ambientes públicos, como no caso do projeto “LidEye” do *sandbox* regulatório recifense, sem criar entraves ou amarras excessivas em um ambiente que visa preservar justamente um maior relaxamento das travas regulatórias para possibilitar a inovação (BIONI, 2021).

313 O autor faz uma ressalva a essa medida, pois apesar de “algumas jurisdições exigem que o participante do programa de *sandbox* contrate seguro para indenizar os investidores em caso de perdas decorrentes do produto ou serviço ofertado. A princípio, tal exigência oneraria em excesso os participantes do programa, de modo que se sugere que tal salvaguarda não seja utilizada como regra geral pelos reguladores no âmbito do *sandbox* brasileiro.

314 Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

315 Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: II - a autodeterminação informativa;

CONSIDERAÇÕES FINAIS

Esse trabalho discutiu como não é possível a regulação de qualquer país prever como se dará a aplicação das novas tecnologias e qual será o seu impacto no tecido social. Para tanto, apontou que o sandbox regulatório pode ser uma ferramenta útil para permitir testes dessas novas tecnologias em ambientes seguros diante do êxito nas experiências realizadas no Setor Financeiro antes de disponibilizar esses produtos ou serviços para o público geral.

Em seguida, discorreu sobre o papel atribuído pela Constituição Federal ao Estado como regulador da atividade econômica nacional e como o Ambiente Regulatório Experimental (*sandbox* regulatório) pode ser mais uma ferramenta útil disponível para os gestores públicos com comprovados efeitos positivos, para atrair novos empreendimentos, incentivando o desenvolvimento local.

Também abordou o conceito de cidade inteligente e como o sandbox regulatório pode ser uma ferramenta de redução de desigualdade social. Assim, o sandbox regulatório pode auxiliar em tornar as cidades brasileiras em cidades inteligentes, reduzindo a desigualdade social através do oferecimento de serviços públicos, antes distantes da parcela mais vulnerável, realizando a inclusão social através da inclusão digital.

Em seguida, tratou sobre a responsabilidade civil e deveres do Poder Público no tratamento de dados pessoais e como a LGPD reconhece a disparidade na relação entre o titular de dados pessoais e a Administração Pública ao prever um capítulo específico sobre as formas e procedimentos em que o gestor público poderá tratar os dados pessoais, impondo o dever de transparência e que o tratamento tenha como objetivo cumprir uma finalidade e interesse público. E, reconhecendo a sensibilidade para esse tipo de tratamento, a ANPD elaborou um Guia Orientativo exclusivo para o tratamento de dados pessoais pelo Poder Público.

Além disso, discorreu sobre a possibilidade de desafiar o entendimento que a Administração Pública não poderia ser alvo

de sanções pecuniárias pelo descumprimento da LGPD diante da ausência de vedação expressa.

Também foi discutido como a ausência de tratamento específico para dados pessoais em ambientes regulatórios experimentais (*sandboxes* regulatórios) e o esforço, ainda que inicial, que haja uma proteção maior para o uso dos dados pessoais nesses ambientes mais desregulados, especialmente quando observamos iniciativas voltadas para a segurança pública, cuja LGPD não possui ingerência enquanto não houver uma lei específica que trate sobre o uso de dados pessoais nessa seara.

Por fim, foram apresentadas algumas sugestões de salvaguardas para obter uma maior proteção dos dados pessoais através de controles previstos nos programas de *sandbox*, sem impor amarras excessivas que possam desnaturar o próprio instituto que prevê, naturalmente, um maior relaxamento das normas reguladoras para incentivar a inovação, especialmente em áreas sensíveis como a segurança pública.

Assim, o *sandbox* regulatório é uma ferramenta importante para auxiliar em tornar as cidades brasileiras em cidades inteligentes, trazendo todos os benefícios dessa transformação digital sem desprezar as normas legais existentes, em especial a Lei Geral de Proteção de Dados.

REFERÊNCIAS

MOORE, Gordon E. **Cramming more components onto integrated circuits**. Eletronic Magazine, Nova Iorque, v. 38, n. 8, p. 114–117, abr. 1965. Republicado com transcrição da entrevista em 2005 pela Intel. Disponível em: https://hasler.ece.gatech.edu/Published_papers/Technology_overview/gordon_moore_1965_article.pdf. Acesso em 26 jun. 2024

JENIK, Ivo; LAUER, Kate. **Regulatory Sandboxes and Financial Inclusion**. CGAP Working Paper. Washington: CGAP, 2017. Disponível em <https://www.cgap.org/sites/default/files/Working-Paper-Regulatory-Sandboxes-Oct-2017.pdf>. Acesso em 27 de junho de 2024.

OCDE, 2023. **Regulatory sandboxes in artificial intelligence**. Disponível em https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/07/regulatory-sandboxes-in-artificial-intelligence_a44aae4f/8f80a0e6-en.pdf. Acesso em 30 de dezembro de 2024.

BRASIL. **Lei Federal nº. 13.874, de 20 de setembro de 2019**. Brasília, DF: Presidência da República, [2019]. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13874.htm. Acesso em 26 de junho de 2024.

BRASIL. **Lei Complementar Federal nº. 182, de 1º de junho de 2021**. Brasília, DF: Presidência da República, [2021]. Disponível em https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp182.htm. Acesso em 27 de junho de 2024.

LIMA, Cíntia Rosa Pereira de (coord.). **Comentários à Lei Geral de Proteção de Dados: Lei n. 13.709/2018, com alterações da lei n. 13.853/2019**. São Paulo: Almedina, 2020.

BRASIL. **Lei Federal nº. 13.709, de 14 de agosto de 2018.** Brasília, DF: Presidência da República, [2018]. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 30 de dezembro de 2024.

V. SHWAB, Klaus. **A quarta revolução industrial.** Edipro: São Paulo, 2016.

BRASIL. **Constituição Federal de 05 de outubro de 1988.** Brasília, DF: Presidência da República, [1988]. Disponível em https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 26 de junho de 2024.

CARVALHO FILHO, José dos Santos. **Manual de Direito Administrativo.** Rio de Janeiro: Lumen Juris, 2009.

FEIGELSON, Bruno; LEITE, Luiza. **Sandbox: experimentalismo no direito exponencial.** São Paulo: RT, 2020.

RIO DE JANEIRO. **Decreto Municipal nº. 50.697 de 26 de abril de 2022.** Disponível em https://doweb.rio.rj.gov.br/apifront/portal/edicoes/imprimir_materia/825386/5322#:~:text=ABRIL%20DE%202022-,Disp%C3%B5e%20sobre%20as%20regras%20provid%C3%A2ncias. Acesso em 16 de julho de 2024.

JOÃO PESSOA. **Lei Municipal nº. 14.092 de 30 de dezembro de 2020.** Disponível em <https://leismunicipais.com.br/a/pb/j/joao-pessoa/lei-ordinaria/2020/1410/14092/lei-ordinaria-n-14092-2020-dispoe-sobre-as-regras-para-constituicao-e-funcionamento-de-ambiente-regulatorio-experimental-sandbox-regulatorio-no-municipio-de-joao-pessoa>. Acesso em 16 de julho de 2024.

RECIFE. **Decreto Municipal nº. 35.511 de 01 de abril de 2022.** Disponível em <http://leismunicipa.is/zdwua>. Acesso em 28 de maio de 2024.

QUIRINO, Carina de Castro; HOCAYEN, Helena Gouvêa de Paula; CUNHA, Marcella Brandão Flores da. **Sandbox regulatório: instrumento experimentalista à disposição da Administração Pública local como suporte ao desenvolvimento econômico.** Revista de Direito Público da Economia – RDPE, Belo Horizonte, ano 21, n. 84, p. 9-33, out./dez. 2023.

OCDE, 2020. **Smart Cities and Inclusive Growth.** Disponível em <https://www.oecd-ilibrary.org/docserver/8a4ce475-en.pdf?expires=1722625010&D>. Acesso em 28 de julho de 2024.

BRASIL. Ministério das Cidades. **Carta Brasileira para Cidades Inteligentes.** Disponível em <https://www.gov.br/cidades/pt-br/aceso-a-informacao/acoes-e-programas/desenvolvimento-urbano-e-metropolitano/projeto-andus/carta-brasileira-para-cidades-inteligentes>. Acesso em 28 de julho de 2024.

BRASIL. Câmara dos Deputados. Disponível em <https://www.camara.leg.br/proposicoesWeb/de,aloc%C3%A1veis%20e%20ncias>. Acesso em 28 de julho de 2024.

ABNT. Associação Brasileira de Normas Técnicas. **ABNT NBR ISO 37122:2020 Cidades e comunidades sustentáveis – Indicadores para cidades inteligentes.** Rio de Janeiro: ABNT, 2020.

ANDRADE, Leandro Teodoro. **Direito da Cidade Inteligente: fundamentos jurídico-econômicos.** São Paulo: RT, 2023.

ANTONIALLI, D. M.; KIRA, B. **Planejamento urbano do futuro, dados do presente: a proteção da privacidade no contexto das cidades inteligentes.** Revista brasileira de estudos urbanos e regionais. v.22, E202003, 2020.

PEREIRA, Caio Mário da Silva. **Instituições de Direito Civil - Vol. III – Contratos.** Rio de Janeiro: Forense, 2014.

TASSO, Fernando Antonio. Capítulo IV. Do Tratamento de Dados Pessoais pelo Poder Público. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). **LGPD: Lei Geral de Proteção de Dados Pessoais comentada**. São Paulo: RT, 2021. p. 261.

BRASIL. Câmara dos Deputados. **Parecer do Relator, Dep. Orlando Silva na Comissão Especial do Projeto de Lei nº. 4.060 de 2012**. Disponível em https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305&. Acesso em 14 de janeiro de 2025.

ALVES, Fabricio da Mota. Capítulo VIII. Da Fiscalização. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). **LGPD: Lei Geral de Proteção de Dados Pessoais comentada**. São Paulo: RT, 2021. p. 416.

BRASIL. Supremo Tribunal Federal. **ADI nº. 6.649 e ADPF nº. 695**. Brasília, DF: Supremo Tribunal Federal, 2022. Disponível em: <https://portal.stf.jus.br/processos/downloadPeca.asp?id=15358978491&ext=.pdf>. Acesso em: 15 de janeiro de 2025.

BRASIL. Câmara dos Deputados. **Projeto de Lei Ordinária nº. 976 de 19 de março de 2021**. Disponível em <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=220AAncias>. Acesso em 13 de janeiro de 2025.

TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. **Tratamento de dados pessoais na LGPD: estudo sobre as bases legais**. Civilistica.com. Rio de Janeiro, a. 9, n. 1, 2020. Disponível em: <<http://civilistica.com/tratamento-de-dados-pessoais-na-lgpd/>>. Data de acesso 13 de janeiro de 2025.

LAB, Laboratório de Inovação Financeira. **Diretrizes gerais para constituição de *sandbox* regulatório no âmbito do mercado financeiro brasileiro**. Disponível em <http://labinovacaofinanceira>.

com/wp-content/uploads/2020/03/Sand_box_lab_vs8_web.pdf. Acesso em 15 de janeiro de 2025.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2021.

10. O USO DA TECNOLOGIA BLOCKCHAIN NO COMBATE À FRAUDE NAS CONTRATAÇÕES PÚBLICAS À LUZ DA LEI Nº 14.133/2021

Desirée Marcelle da Cunha

Advogada. Assessora jurídica na Secretaria de Estado de Educação do Rio de Janeiro. Bacharel em Direito pela Universidade do Estado do Rio de Janeiro (UERJ). Especialista em Direito Digital pelo Instituto de Tecnologia e Sociedade do Rio de Janeiro – ITS Rio em parceria com o Centro de Estudos e Pesquisas no Ensino do Direito da Universidade do Estado do Rio de Janeiro (CEPED/UERJ).

INTRODUÇÃO

A Lei nº 14.133/2021 inaugurou um novo marco normativo para as contratações públicas no Brasil, promovendo não apenas a substituição do regime anterior de licitações, mas também uma inflexão relevante na forma como o Estado concebe a gestão, o controle e a governança de seus processos de contratação. Entre as inovações introduzidas, destaca-se a valorização expressa do planejamento, da transparência e da adoção de soluções tecnológicas como instrumentos voltados ao aumento da eficiência administrativa, à mitigação de riscos e ao fortalecimento da integridade nas compras públicas.

Além disso, o tema em questão apresenta grande relevância, dado que as contratações públicas assumem papel central na dinâmica estatal, na medida em que movimentam parcela significativa do Produto Interno Bruto (PIB) nacional e constituem importante mecanismo de implementação de políticas públicas. Em razão de sua relevância econômica e social, tais procedimentos devem observar, de forma rigorosa, princípios como a legalidade, a moralidade, a publicidade e a eficiência, especialmente em um contexto historicamente marcado por assimetrias informacionais, elevada discricionariedade e recorrentes episódios de desvios e irregularidades.

É nesse cenário que a tecnologia blockchain emerge como um potencial instrumento de aprimoramento da governança pública, uma vez que oferece mecanismos capazes de ampliar a rastreabilidade, a imutabilidade e a auditabilidade dos atos administrativos. Nesse sentido, sua aplicação revela-se particularmente relevante para enfrentar a chamada “opacidade da fase interna” das contratações públicas, uma vez que essa etapa é tradicionalmente desenvolvida em ambientes pouco acessíveis ao controle social e institucional, o que significa que a ausência de registros transparentes pode favorecer ajustes retroativos, direcionamentos indevidos e fragilização dos mecanismos de controle.

Diante disso, o presente artigo tem por objetivo analisar a incorporação da tecnologia blockchain ao sistema normativo estabelecido pela Lei nº 14.133/2021, examinando suas potencialidades e limitações como instrumento de reforço à transparência, à integridade e à conformidade das contratações públicas, em especial no que tange à prevenção à fraude.

Para tanto, adotou-se uma abordagem qualitativa, fundamentada em revisão bibliográfica, análise documental de legislações e relatórios institucionais, bem como no exame de experiências nacionais e internacionais de aplicação da tecnologia blockchain em compras públicas.

Busca-se, com isso, contribuir para o debate jurídico acerca do potencial da blockchain como instrumento de prevenção, detecção e mitigação de fraudes nas contratações públicas, demonstrando de que forma seus mecanismos de imutabilidade, rastreabilidade e auditabilidade podem fortalecer os sistemas de controle, reduzir oportunidades de práticas ilícitas e ampliar a transparência e a integridade dos procedimentos licitatórios, em consonância com a proteção do interesse público e com as diretrizes da Lei nº 14.133/2021.

1. CONTRATAÇÕES PÚBLICAS NO BRASIL

A licitação pública constitui um procedimento administrativo destinado a assegurar à Administração Pública a seleção da proposta mais vantajosa, em consonância com princípios constitucionais fundamentais, como a legalidade, a isonomia, a moralidade e a impessoalidade. Todavia, como é amplamente reconhecido, trata-se de um ambiente permeado por assimetrias de informação, elevada discricionariedade administrativa e múltiplas interações entre agentes públicos e privados, circunstâncias que, não raras vezes, favorecem desvios de finalidade, direcionamento de certames e outras práticas incompatíveis com o interesse público.

Nesse sentido, justamente por sua natureza estratégica, as contratações públicas apresentam elevada vulnerabilidade a práticas corruptivas, ao mesmo tempo em que desempenham papel central na implementação de políticas públicas. Por meio desses procedimentos, os entes governamentais, em diferentes níveis da federação, adquirem bens, serviços e obras essenciais, que vão desde grandes projetos de infraestrutura até insumos indispensáveis para setores como saúde e educação. Assim, a relevância econômica e social das contratações públicas reforça a necessidade de mecanismos robustos de transparência, controle e governança.

Segundo estudos do *World Economic Forum*³¹⁶, em escala global, os gastos governamentais com contratações públicas alcançam cifras expressivas, estimadas em aproximadamente 9,5 trilhões de dólares.

No entanto, esses processos são frequentemente caracterizados por elevada complexidade, limitações de transparência e ampla margem de atuação discricionária por parte dos agentes envolvidos, fatores que aumentam significativamente os riscos de desvios e irregularidades. Estimativas apontam ainda que uma parcela

316 World Economic Forum. *Exploring Blockchain Technology for Government Transparency: Blockchain-Based Public Procurement to Reduce Corruption*. Disponível em: https://www3.weforum.org/docs/WEF_Blockchain_Government_Transparency_Report.pdf. Acesso em 20 jan. 2026.

relevante do valor dos contratos públicos, variando entre 10% e 30%, é comumente comprometida por práticas corruptas, evidenciando a necessidade de instrumentos eficazes de governança e controle³¹⁷.

De modo geral, os contratos governamentais de maior porte seguem um conjunto de etapas sucessivas, que incluem o planejamento da contratação, a apresentação das propostas, a análise e o julgamento das ofertas, e a execução do contrato acompanhada de mecanismos de fiscalização. Em alguns casos, especialmente em contratos de menor valor ou de elevada complexidade técnica, podem ser adotados procedimentos diretos ou negociados. Cada uma dessas fases, no entanto, apresenta vulnerabilidades próprias, que podem abrir espaço para práticas ilícitas, como subornos, interferências indevidas, conluio entre particulares, manipulação de propostas e avaliações fraudulentas.

Diante desse cenário, evidencia-se a necessidade de instrumentos capazes de mitigar as fragilidades estruturais das contratações públicas, especialmente no que se refere à prevenção de fraudes e ao fortalecimento da transparência e da governança administrativa. Nesse contexto, a tecnologia blockchain apresenta-se como uma ferramenta promissora de combate a práticas ilícitas, ao viabilizar o registro imutável, rastreável e verificável de todas as decisões e atos praticados ao longo do procedimento licitatório. Ao reduzir a assimetria informacional, restringir intervenções discricionárias indevidas e ampliar significativamente a capacidade de controle e auditoria pelos órgãos competentes e pela sociedade, essa tecnologia contribui para a integridade dos processos licitatórios, promovendo maior transparência, eficiência e alinhamento ao interesse público, além de fortalecer a confiança institucional na gestão dos recursos estatais.

317 Ibid.

2. A TECNOLOGIA BLOCKCHAIN COMO INSTRUMENTO DE TRANSPARÊNCIA, GOVERNANÇA E PREVENÇÃO À FRAUDE

A tecnologia blockchain ganhou notoriedade a partir de sua vinculação ao Bitcoin, criptomoeda apresentada em 2008 como alternativa aos sistemas financeiros tradicionais, criada por um programador anônimo sob o pseudônimo de Satoshi³¹⁸. Nesse primeiro momento, o blockchain desempenhava a função de estrutura técnica responsável por registrar e validar as transações realizadas no ambiente digital da moeda, assegurando a confiabilidade do sistema sem a necessidade de uma autoridade central.

Segundo Melanie Swan³¹⁹, esse mecanismo pode ser compreendido como um livro-razão de acesso público, no qual as transações são registradas de forma contínua e encadeada. Assim, cada conjunto de registros forma um bloco que, após validado por meio de um processo de consenso conhecido como mineração, passa a integrar a cadeia de dados e a lógica de encadeamento entre os blocos impede alterações posteriores sem que todo o sistema seja afetado, conferindo elevado grau de segurança às informações armazenadas.

Nesse contexto, registre-se que a blockchain do Bitcoin, conforme proposta por Nakamoto, destinava-se exclusivamente ao registro de transações de natureza monetária, não comportando a inserção de condições mais complexas ou lógicas programáveis. Nesse modelo, a tecnologia funcionava como uma infraestrutura segura para a transferência de valores, mas com aplicações limitadas do ponto de vista funcional.

318 LEITÃO, Andre Studart; FERREIRA, Hélio Rios. AS NOVAS TECNOLOGIAS A SERVIÇO DA NOVA ADMINISTRAÇÃO: A BLOCKCHAIN, OS SMART CONTRACTS E A NOVA LEI DE LICITAÇÕES E CONTRATOS (LEI Nº 14.133/2021). *Revista de Direito Brasileira*, Florianópolis, Brasil, v. 29, n. 11, p. 73, 2022. DOI: 10.26668/IndexLawJournals/2358-1352/2021.v29i11.7493. Disponível em: <https://www.indexlaw.org/index.php/rdb/article/view/7493>. Acesso em: 27 jan. 2026.

319 SWAN, Melanie. *Blockchain: Blueprint for a New Economy*. Sebastopol, California: O'Reilly Media Inc., 2015. 149 p.

Essa perspectiva começou a se expandir em 2013, quando Vitalik Buterin apresentou o Ethereum, plataforma voltada ao desenvolvimento de aplicações descentralizadas. Com a introdução dos contratos inteligentes (*smart contracts*), a blockchain passou a possibilitar a execução automática e confiável de códigos previamente acordados entre as partes, sem a necessidade de intermediários. Assim, embora Ethereum, assim como o Bitcoin, se baseie em uma rede blockchain, ele se diferencia por viabilizar não apenas a transferência de valores, mas também a criação e execução de programas autoexecutáveis capazes de operar conforme termos previamente definidos, ampliando significativamente o leque de aplicações da tecnologia.³²⁰

Essa ampliação funcional torna-se particularmente relevante no contexto das contratações públicas, caracterizadas por procedimentos formais, sucessão de atos administrativos e observância estrita de regras pré-estabelecidas.

A utilização de contratos inteligentes permite conceber modelos nos quais determinadas condições legais e cláusulas contratuais sejam estruturadas e executadas automaticamente, conferindo maior previsibilidade e segurança ao processo. Mais do que uma inovação tecnológica, trata-se de um instrumento capaz de reforçar a rastreabilidade dos atos praticados, dificultar alterações indevidas e reduzir espaços de opacidade, especialmente nas fases menos visíveis do procedimento.

Portanto, embora a arquitetura blockchain tenha se originado no contexto das criptomoedas, seu potencial de aplicação vai muito além desse campo. Com o amadurecimento da tecnologia, ela passou a ser explorada em diferentes setores, justamente por sua capacidade de assegurar integridade, rastreabilidade e transparência dos registros, atributos que despertam particular interesse em áreas como as contratações públicas.

320 MASCARENHAS, Juliana Z. G.; VIEIRA, Alex B.; ZIVIANI, Artur. **Análise da Rede de Transações do Ethereum**. In: workshop em blockchain: teoria, tecnologias e aplicações (wblockchain), 1., 2018, Campos do Jordão. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2018. Disponível em: <https://sol.sbc.org.br/index.php/wblockchain/article/view/2352/2316>. Acesso em: 12 jan. 2026.

Nesse contexto, merece destaque a iniciativa do *World Economic Forum* (WEF), que lançou o projeto *Unlocking Government Transparency with Blockchain Technology*³²¹, voltado à redução de práticas corruptivas e ao aprimoramento dos mecanismos de seleção de fornecedores no âmbito das contratações públicas. A proposta parte do reconhecimento de que a corrupção compromete a economia e fragiliza a confiança da sociedade nas instituições públicas, inclusive nos sistemas tradicionais de compras governamentais. Dessa forma, a adoção da blockchain permite estender o registro seguro e rastreável a diversas fases do procedimento, desde a divulgação dos editais até a execução contratual.

Contudo, a adoção da tecnologia blockchain nas compras públicas não está isenta de desafios. Entre os principais pontos de atenção, destacam-se as questões relacionadas à proteção de dados e à capacidade de escalabilidade dos sistemas, especialmente diante do elevado volume de informações e transações envolvidas nos processos de contratação.

Soma-se a isso o problema das desigualdades digitais, uma vez que a participação em estruturas baseadas em blockchain pressupõe acesso à tecnologia e domínio técnico mínimo por parte dos usuários, ao passo que a Administração Pública demanda investimentos financeiros, organizacionais e institucionais para viabilizar sua implementação.

Diante desse cenário, o *World Economic Forum* tem apontado como alternativa mais promissora os modelos de blockchain híbridos ou permissionados, que limitam o número de participantes e conciliam maior controle institucional com registros transparentes e rastreáveis das transações.³²²

321 World Economic Forum. **Exploring Blockchain Technology for Government Transparency: Blockchain-Based Public Procurement to Reduce Corruption.** Disponível em: https://www3.weforum.org/docs/WEF_Blockchain_Government_Transparency_Report.pdf. Acesso em 20 jan. 2026.

322 Bustamante P, Cai M, Gomez M, Harris C, Krishnamurthy P, Law W, Madison MJ, Murtazashvili I, Murtazashvili JB, Mylovanov T, Shapoval N, Vee A and Weiss M (2022) Government by Code? Blockchain Applications to Public Sector Governance. *Front. Blockchain* 5:869665. doi: 10.3389/fbloc.2022.869665.

Apesar dos desafios, a blockchain apresenta grande potencial para ampliar a transparência e a rastreabilidade nos procedimentos licitatórios, contribuindo para a prevenção de fraudes e práticas corruptas, inclusive na fase interna. Sua utilização é particularmente relevante na elaboração de editais e na pesquisa de preços, pois a rede blockchain atua como um livro-razão imutável, assegurando a integridade e a confiabilidade das informações registradas.

Ou seja, a arquitetura descentralizada dessa tecnologia permite que os registros sejam distribuídos e validados por múltiplos participantes autorizados do sistema, assegurando a integridade, a imutabilidade e a rastreabilidade das informações ali inseridas. Tal característica reduz significativamente o risco de alterações indevidas, manipulações posteriores ou supressão de dados relevantes, promovendo um ambiente de elevada transparência e confiabilidade.

Nesse contexto, cada etapa do planejamento da contratação permanece registrada de forma cronológica e auditável, fortalecendo os mecanismos de controle interno e externo e conferindo maior legitimidade às decisões administrativas adotadas antes mesmo da publicação do edital.

Aliás, a tecnologia blockchain estabelece um diálogo direto com os princípios consagrados na Lei nº 14.133/2021, que consagra o planejamento como eixo central das contratações públicas. O novo marco legal reforça a exigência de decisões administrativas devidamente fundamentadas, lastreadas em estudos técnicos preliminares, pesquisa de preços consistente e adequada gestão de riscos, em harmonia com os princípios da transparência, probidade administrativa, legalidade e eficiência.

Nesse sentido, a adoção de soluções baseadas em blockchain também se alinha aos objetivos da Lei do Governo Digital (Lei nº 14.129/2021), ao contribuir para o incremento da eficiência administrativa por meio da desburocratização de procedimentos, do estímulo à inovação e do avanço da transformação digital no âmbito da Administração Pública.

Todavia, dentre as inúmeras facilidades trazidas pela adoção da tecnologia blockchain nas contratações públicas, é importante destacar a sua especial relevância para a fase interna do procedimento, atuando como importante instrumento de prevenção a práticas de conluio e à ocorrência de sobrepreço. Ao registrar, em um sistema distribuído e auditável, todos os atos preparatórios, como contatos com fornecedores, estudos técnicos, justificativas para definição do objeto e formação do preço estimado, a tecnologia amplia a rastreabilidade das decisões administrativas e reduz o espaço para direcionamentos indevidos.³²³

Além disso, a integração de diferentes órgãos e entes federativos em uma mesma infraestrutura possibilita a consolidação de dados sobre contratos, fornecedores e valores praticados, mitigando a atual fragmentação informacional. Esse ambiente favorece a identificação de discrepâncias de preços em contratações semelhantes e fortalece os mecanismos de controle preventivo, contribuindo para maior integridade, transparência e eficiência nas contratações públicas.³²⁴

Por esse motivo, é amplamente reconhecido o papel central desta tecnologia como mecanismo de prevenção a condutas ilícitas, tais como a corrupção, a má gestão de recursos, acordos indevidos e diferentes modalidades de fraude, que frequentemente resultam em prejuízos ao erário e na ineficiência da implementação de políticas públicas³²⁵.

Nesse contexto, a aplicação da tecnologia blockchain no setor público destaca-se por favorecer a prestação de serviços estatais de forma mais segura e eficiente, ao mesmo tempo em que amplia a

323 FERNANDES, Ketlyn Gonçalves. Corrupção e opacidade nas contratações públicas: a necessidade de uma fase interna transparente via tecnologia blockchain. In: ZOCKUN, Maurício; GABARDO, Emerson (coord.). **Novas leis: promessas de um futuro melhor? Livro do XXXVI Congresso Brasileiro de Direito Administrativo**. Belo Horizonte: Fórum, 2023. p. 361-378. ISBN 978-65-5518-581-2. Disponível em: https://ibda.com.br/wp-content/uploads/2024/10/EmersonGabardo_Etal_NovasLeis_MIOLO_GRAFICA.pdf#page=361. Acesso em: 29 jan. 2026.

324 Ibid.

325 ZILIOTTO, M. M. **Tecnologia Blockchain nas Contratações Públicas no Brasil**. Belo Horizonte: Fórum, 2022.

automação de processos e fortalece a rastreabilidade e a capacidade de auditoria dos atos administrativos, com reflexos positivos diretos para a coletividade.³²⁶

No âmbito nacional, destaca-se a iniciativa do Tribunal de Contas da União, em parceria com o Banco Nacional de Desenvolvimento Econômico e Social, voltada à institucionalização do uso da tecnologia blockchain no setor público. Trata-se da Rede Blockchain Brasil (RBB), uma rede de abrangência nacional estruturada com base em um modelo próprio de governança e em uma infraestrutura tecnológica compartilhada, cujo principal objetivo é viabilizar e estimular a adoção de soluções baseadas em blockchain para aplicações de interesse público.

Formalizada por meio de Acordo de Cooperação firmado em abril de 2022, a RBB busca racionalizar recursos, reduzir custos e eliminar barreiras à inovação tecnológica na Administração Pública. Além disso, permite a adesão de outros órgãos e entidades por meio de procedimentos específicos de governança, reforçando seu caráter colaborativo e interinstitucional³²⁷. Nesse contexto de busca por maior transparência, governança e racionalização dos procedimentos administrativos, a iniciativa do Tribunal de Contas da União revela-se especialmente alinhada às reflexões até aqui desenvolvidas.

A criação da Rede Blockchain Brasil (rede público-permissionada)³²⁸, em parceria com o BNDES, foi inspirada em

326 TCU – Tribunal de Contas da União. **Sumário Executivo:** levantamento da tecnologia blockchain. Acórdão 1.613/2020-TCU-Plenário. Relator Ministro Aroldo Cedraz. Brasília: TCU, Secretária das Sessões (Seses), 2020. Disponível em: <https://portal.tcu.gov.br/levantamento-da-tecnologia-blockchain.htm>. Acesso em: 28 jan 2026.

327 Brasil. Rede Blockchain Brasil. *INFRAESTRUTURA E GOVERNANÇA PARA EXECUÇÃO DE APLICAÇÕES DE INTERESSE PÚBLICO*. Brasília, 2025. DOI: 10.5281/zenodo.17701100. Disponível em: https://portal.tcu.gov.br/uploads/Rede_Blockchain_Brasil_Publicacao_Infraestrutura_e_Governanca_727da4d44f.pdf. Acesso em: 29 jan. 2026.

328 Segundo a Cartilha apresentada pelo TCU, “a RBB, é pública porque pode ser acessada por qualquer pessoa ou entidade, sem a necessidade de autorização prévia, e permissionada porque apenas entidades previamente conhecidas e confiáveis podem registrar dados na blockchain”.

experiências internacionais como a LACChain - rede para a América Latina liderada pelo BID, Alastria e EBSI (*European Blockchain Service Infrastructure*) e materializa, no plano institucional, a possibilidade concreta de utilização da tecnologia blockchain como instrumento de apoio às contratações públicas e a outras políticas de interesse coletivo.

Ora, ao propor uma infraestrutura tecnológica compartilhada, dotada de modelo próprio de governança e aberta à adesão de múltiplas instituições, a RBB dialoga diretamente com os princípios da Lei nº 14.133/2021 e com as diretrizes do Governo Digital, ao buscar reduzir custos, otimizar recursos e fomentar a inovação no setor público. Trata-se, portanto, de um movimento que ultrapassa o campo teórico e sinaliza um esforço coordenado do Estado brasileiro no sentido de incorporar soluções tecnológicas capazes de fortalecer o controle, a transparência e a eficiência administrativa, especialmente em ambientes sensíveis como o das contratações públicas.

Já no âmbito internacional, a Estônia é um exemplo emblemático, pois o país desenvolveu uma infraestrutura digital integrada conhecida como *e-Estonia*, por meio da qual são interligados diversos sistemas estatais, incluindo os setores de justiça, saúde, segurança, atividade legislativa e relações comerciais. No campo legislativo, destaca-se a utilização do sistema *e-Law*, que emprega tecnologia blockchain para assegurar o acesso público a informações relacionadas aos projetos de lei apresentados no país desde 2003, valendo-se de sua própria blockchain, a KSI.³²⁹

No âmbito das contratações públicas da Estônia, essa lógica de digitalização e interoperabilidade também se manifesta por meio do *Riigihangete Register* (Registro de Compras Públicas), plataforma centralizada que concentra todos os procedimentos licitatórios realizados pelas instituições do setor público estoniano, incluindo o governo central, os municípios e as empresas estatais.

329 CASALLAS, Jenny Alexandra Triana; LOVELLE, Juan Manuel Cueva; MOLANO, Jose Ignacio Rodriguez. Smart contracts with blockchain in the public sector. *International Journal of Interactive Multimedia and Artificial Intelligence*, La Rioja: Universidad Internacional de La Rioja, 2020. Disponível em: https://www.ijimai.org/journal/sites/default/files/2020-08/ijimai_6_3_8.pdf. Acesso em: 19 jan. 2026.

O sistema estoniano permite a divulgação eletrônica dos avisos de licitação, o acesso às informações essenciais sobre os contratos, bem como a identificação das autoridades contratantes e das empresas participantes, assegurando elevado grau de transparência e rastreabilidade ao longo de todo o procedimento. Ademais, a possibilidade de submissão eletrônica de propostas contribui para a simplificação dos processos, a redução da carga administrativa e o aumento da eficiência das compras públicas, evidenciando como o uso de tecnologias digitais, inclusive soluções baseadas em blockchain, pode fortalecer a governança e o controle das contratações estatais.

Essa abordagem digital, aliada à transparência proporcionada pelas soluções baseadas em blockchain, reflete-se nos baixos índices de corrupção do país, que figura em posições elevadas no Índice de Percepção da Corrupção (CPI) da Transparency International (2023)³³⁰, demonstrando a relação positiva entre governança digital e integridade pública.

Diante do exposto, verifica-se que a tecnologia blockchain desponta como instrumento estratégico de fortalecimento da transparência, da governança e, sobretudo, da prevenção à fraude nas contratações públicas. Sua evolução ampliou significativamente as possibilidades de aplicação para além do mercado financeiro, permitindo não apenas a automação de procedimentos, mas também o registro imutável, rastreável e auditável dos atos administrativos, desde a fase interna até a execução contratual.

Dessa forma, ao reduzir a assimetria informacional, limitar espaços para intervenções discricionárias indevidas e potencializar os mecanismos de controle e fiscalização, a blockchain revela-se capaz de mitigar práticas ilícitas, contribuindo para processos licitatórios mais íntegros, eficientes e alinhados ao interesse público.

Embora persistam desafios relacionados à proteção de dados, à escalabilidade e à inclusão digital, as experiências nacionais e

330 Transparency International, Corruption perceptions index: Explore the results”, 2023. Disponível em: <https://www.transparency.org/en/cpi/2023>. Acesso em 29 jan. 2026.

internacionais analisadas demonstram que modelos permissionados ou híbridos são capazes de compatibilizar os benefícios da descentralização com as exigências próprias da Administração Pública. Assim, a adoção responsável e institucionalmente estruturada da blockchain revela-se alinhada aos princípios consagrados na Lei nº 14.133/2021 e às diretrizes do Governo Digital, constituindo-se em ferramenta promissora para a prevenção de fraudes, o incremento da confiança institucional e a promoção do interesse público nas contratações estatais.

CONSIDERAÇÕES FINAIS

À luz das reflexões desenvolvidas, constata-se que a tecnologia blockchain apresenta elevado potencial como ferramenta de prevenção à fraude nas contratações públicas, ao enfrentar fragilidades estruturais historicamente associadas a esses procedimentos, especialmente aquelas decorrentes da assimetria informacional, da excessiva discricionariedade administrativa e da opacidade que ainda marca determinadas fases do processo licitatório.

Assim, ao permitir o registro distribuído, imutável, rastreável e permanentemente auditável dos atos administrativos, a blockchain promove maior transparência e confiabilidade nas decisões estatais, contribuindo para a mitigação de práticas como conluios, direcionamentos indevidos e manipulações procedimentais, em consonância com o interesse público.

Sob essa perspectiva, a incorporação da blockchain às contratações públicas não deve ser compreendida apenas como inovação tecnológica, mas como um instrumento de fortalecimento da governança administrativa, ao ampliar os mecanismos de controle, fiscalização e responsabilização, tanto por parte dos órgãos institucionais quanto da sociedade. Ao reduzir espaços de intervenção indevida e ampliar a capacidade de auditoria, essa tecnologia revela-se compatível com os princípios da transparência, da integridade,

da eficiência e do controle, expressamente consagrados pela Lei nº 14.133/2021.

Não obstante, o estudo evidencia que a adoção da blockchain no setor público demanda cautela e adequada conformação jurídico-institucional. Desafios relacionados à proteção de dados pessoais, à escalabilidade dos sistemas, à inclusão digital e à definição de modelos de governança tecnológica compatíveis com o regime jurídico-administrativo impõem limites à utilização indiscriminada de redes públicas e não permissionadas.

Nesse sentido, as experiências analisadas indicam que soluções permissionadas ou híbridas se mostram mais adequadas às contratações públicas, ao conciliarem os benefícios da tecnologia com as exigências de segurança jurídica, controle e responsabilização administrativa.

Por fim, iniciativas como a Rede Blockchain Brasil, assim como experiências internacionais consolidadas, a exemplo do modelo estoniano, demonstram que a utilização da blockchain nas contratações públicas é viável e compatível com o arcabouço normativo brasileiro, em especial com a Lei nº 14.133/2021 e com as diretrizes da Lei do Governo Digital.

Conclui-se, portanto, que a adoção responsável, gradual e juridicamente orientada da tecnologia blockchain pode contribuir de forma significativa para o aprimoramento da transparência, da governança e da prevenção de fraudes nas contratações públicas, fortalecendo a confiança institucional e promovendo uma Administração Pública mais íntegra, eficiente e orientada à prevenção.

REFERÊNCIAS

BRASIL. Rede Blockchain Brasil. Infraestrutura e governança para execução de aplicações de interesse público. Brasília, 2025. DOI: 10.5281/zenodo.17701100. Disponível em: https://portal.tcu.gov.br/uploads/Rede_Blockchain_Brasil_Publicacao_Infraestrutura_e_Governanca_727da4d44f.pdf. Acesso em: 29 jan. 2026.

BUSTAMANTE, P.; CAI, M.; GOMEZ, M.; HARRIS, C.; KRISHNAMURTHY, P.; LAW, W.; MADISON, M. J.; MURTAZASHVILI, I.; MURTAZASHVILI, J. B.; MYLOVANO, T.; SHAPOVAL, N.; VEE, A.; WEISS, M. Government by Code? Blockchain Applications to Public Sector Governance. *Frontiers in Blockchain*, v. 5, p. 869665, 2022. doi: 10.3389/fbloc.2022.869665.

CASALLAS, Jenny Alexandra Triana; LOVELLE, Juan Manuel Cueva; MOLANO, Jose Ignacio Rodriguez. Smart contracts with blockchain in the public sector. *International Journal of Interactive Multimedia and Artificial Intelligence*, La Rioja: Universidad Internacional de La Rioja, 2020. Disponível em: https://www.ijimai.org/journal/sites/default/files/2020-08/ijimai_6_3_8.pdf. Acesso em: 19 jan. 2026.

FERNANDES, Ketlyn Gonçalves. Corrupção e opacidade nas contratações públicas: a necessidade de uma fase interna transparente via tecnologia blockchain. In: ZOCKUN, Maurício; GABARDO, Emerson (coord.). *Novas leis: promessas de um futuro melhor?* Livro do XXXVI Congresso Brasileiro de Direito Administrativo. Belo Horizonte: Fórum, 2023. p. 361-378. ISBN 978-65-5518-581-2. Disponível em: https://ibda.com.br/wp-content/uploads/2024/10/EmersonGabardo_Etal_NovasLeis_MIOLO_GRAFICA.pdf#page=361. Acesso em: 29 jan. 2026.

LEITÃO, Andre Studart; FERREIRA, Hélio Rios. As novas tecnologias a serviço da nova administração: a blockchain, os smart contracts e a nova Lei de Licitações e Contratos (Lei nº 14.133/2021). *Revista de*

Direito Brasileira, Florianópolis, v. 29, n. 11, p. 73, 2022. DOI: 10.26668/IndexLawJournals/2358-1352/2021.v29i11.7493. Disponível em: <https://www.indexlaw.org/index.php/rdb/article/view/7493>. Acesso em: 27 jan. 2026.

MASCARENHAS, Juliana Z. G.; VIEIRA, Alex B.; ZIVIANI, Artur. Análise da rede de transações do Ethereum. In: *Workshop em Blockchain: teoria, tecnologias e aplicações (WBlockchain)*, 1., 2018, Campos do Jordão. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2018. Disponível em: <https://sol.sbc.org.br/index.php/wblockchain/article/view/2352/2316>. Acesso em: 12 jan. 2026.

SWAN, Melanie. *Blockchain: Blueprint for a New Economy*. Sebastopol, California: O'Reilly Media Inc., 2015. 149 p.

TCU – Tribunal de Contas da União. Sumário executivo: levantamento da tecnologia blockchain. Acórdão 1.613/2020-TCU-Plenário. Relator Ministro Aroldo Cedraz. Brasília: TCU, Secretaria das Sessões (Seses), 2020. Disponível em: <https://portal.tcu.gov.br/levantamento-da-tecnologia-blockchain.htm>. Acesso em: 28 jan. 2026.

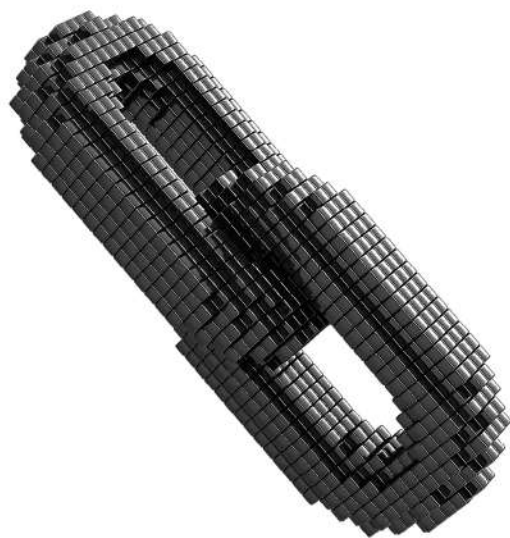
TRANSPARENCY INTERNATIONAL. *Corruption perceptions index: Explore the results*, 2023. Disponível em: <https://www.transparency.org/en/cpi/2023>. Acesso em: 29 jan. 2026.

WORLD ECONOMIC FORUM. *Exploring Blockchain Technology for Government Transparency: Blockchain-Based Public Procurement to Reduce Corruption*. Disponível em: https://www3.weforum.org/docs/WEF_Blockchain_Government_Transparency_Report.pdf. Acesso em: 20 jan. 2026.

ZILIOOTTO, M. M. *Tecnologia Blockchain nas Contratações Públicas no Brasil*. Belo Horizonte: Fórum, 2022.

PARTE IV

GOVERNANÇA REGULATÓRIA,
INTELIGÊNCIA ARTIFICIAL E
DIREITOS FUNDAMENTAIS



11. METARREGULAÇÃO E ESTRATÉGIA REGULATÓRIA DA AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS: EXPERIÊNCIAS E DESAFIOS

Felipe Tavares de Assis

Especialista em Direito Digital pelo Instituto de Tecnologia e Sociedade do Rio de Janeiro – ITS Rio em parceria com o Centro de Estudos e Pesquisas no Ensino do Direito da Universidade do Estado do Rio de Janeiro (CEPED/ UERJ). Possui graduação em Rechtswissenschaft (Jura) pela Universität Passau (2022) e graduação em Direito pela Universidade de São Paulo (2022).

INTRODUÇÃO

O conceito de metarregulação pode ser analisado como uma “regulação sobre a autorregulação da indústria”, em que órgãos reguladores estatais realizam uma análise de práticas dos entes regulados, para aferição da conformidade em determinados temas³³¹. A metarregulação tem feito parte da estratégia regulatória adotada pela Lei Geral de Proteção de Dados – LGPD e liderado pela Agência Nacional de Proteção de Dados – ANPD –; o trabalho a ser realizado pretenderá analisar criticamente esta opção regulatória no contexto de proteção de dados pessoais.

A tendência regulatória no ordenamento jurídico tem, em larga escala, adotado a metarregulação como estratégia regulatória em diversos setores, como valorização dos valores de eficácia e participação social, exemplificadamente.

Igual tendência se manifesta por meio do panorama regulatório introduzido pela LGPD, que atribui à ANPD o protagonismo na condução da estratégia regulatória em matéria de proteção de dados,

331 GRABOSKY, Peter. Meta-regulation. In: DRAHOS, Peter. *Regulatory Theory: Foundations and applications*. 2017, ANU Press, Canberra, p.1.

que compreende a participação e colaboração de diversos setores da sociedade, especialmente dos entes regulados.

A partir de uma análise do histórico regulatório da ANPD em matéria de proteção de dados, é possível compreender de forma mais precisa a (in)eficácia de uma estratégia metarregulatória, bem como estabelecer pontos de atenção e considerações pertinentes.

No Capítulo 1, o conceito de metarregulação é analisado a partir de sua origem, contexto político e econômico e possíveis limitações de sua aplicação. No Capítulo 2, a metarregulação é compreendida à luz da estratégia regulatória de proteção de dados no ordenamento jurídico brasileiro e dos principais instrumentos regulatórios adotados pelo legislador. O Capítulo 3 apresenta uma análise geral da função desempenhada pela ANPD, como pilar do arcabouço regulatório; examinam-se a agenda regulatória da agência e suas normas, publicações e iniciativas. O Capítulo 4 estabelece uma revisão crítica dos achados desta análise, traduzindo-os em possíveis lacunas, limites regulatórios e pontos de melhoria.

A metodologia do trabalho envolve a revisão bibliográfica dos conceitos apontados e a análise documental de atos normativos, publicações e documentos públicos da ANPD e de outras entidades governamentais e setoriais.

1. O CONCEITO DE METARREGULAÇÃO.

1.1 Contornos gerais da metarregulação.

Em obra fundamental dos estudos contemporâneos acerca de regulação e sua relação com novas tecnologias, Lawrence Lessig traz a afirmação de que “*code is law*”. Ao analisar a evolução do ambiente cibernético na virada do século, o constitucionalista percebe que o mundo atual é marcado por uma predominância da tecnologia (código), que coexiste junto ao direito como eixo normativo. No capítulo introdutório de seu livro, Lessig consigna que

*in real space we recognize how laws regulate – through constitutions, statutes, and other legal codes. In cyberspace we must understand how code regulates – how the software and hardware that make cyberspace what it is regulate cyberspace. As William Mitchell puts it, this code is cyberspace’s ‘law’. Code is law*³³².

Para Lessig, a regulação da tecnologia se dá mediante quatro modalidades complementares: leis e normas, mercado e arquitetura física, e a eficácia da regulação depende, essencialmente, da harmonização entre estes quatro fatores³³³.

O conceito de metarregulação dialoga diretamente com o cenário da ausência de monopólio regulador do Estado³³⁴. Demonstra traços típicos de um sistema de regulação descentralizada, pautando-se em uma perspectiva regulatória distanciada do modelo tradicional de regulação centralizado na figura do Estado, como instituição detentora do monopólio da força, capaz de compreender a realidade social na integridade e influenciar o comportamento do todo social a partir da edição de normas³³⁵.

Trata-se, mais especificamente, de estratégia na qual o Estado regula não diretamente a conduta final dos regulados, mas a forma

332 LESSIG, LAWRENCE. *Code and other laws of cyberspace*. Nova Iorque: Basic Books, 1999, p. 6.

333 KLITOU, Demetrius. *Privacy-Invasive Technologies and Privacy by Design: Safeguarding Privacy, Liberty and Security in the 21st Century*. Leiden University: T.M.C. Asser Press, 2014.

334 Destaca-se desde já a ausência de um conceito incontestado de metarregulação, sendo definido com contornos mais ou menos restritos. Nesse sentido, mencionando Coglianese e Mendelson, Verbruggen e Havinga apontam que “while for some scholars the concept is linked to the ‘state’s oversight on self-regulatory arrangements’, for others the concept is wider and involves the use of control and steering mechanisms between different regulatory actors and levels of regulation”. VERBRUGGEN, Paul; HAVINGA, Tetty. *The Rise of Transnational Private Meta-Regulators*. *Tillburg Law Review* v. 21, p. 119, 2016. Uma análise exaustiva das diferentes acepções de metarregulação extrapola o escopo do presente trabalho, razão pela qual serão examinados somente os contornos gerais do conceito.

335 Segundo Black, o conceito de regulação descentralizada ou policêntrica pode ser obtido em contraposição ao conceito de regulação pelo Estado, o qual assume tradicionalmente uma lógica de comando e controle, por meio da prescrição de condutas e imposição de sanções. BLACK, Julia. *Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a ‘Post-Regulatory’ World*. *Current Legal Problems* v. 54, p. 105, 2001.

como estes se autorregulam. Compreende uma justaposição entre o campo regulatório imediato – autorregulação pelo agente responsável pela atividade regulada – e o mediato – definição de princípios, padrões-mínimos de conformidade, guia de procedimentos, avaliação de conformidade e prestação de contas.

Grabosky define-a como um conjunto de abordagens em que a autoridade pública procura regular a autorregulação, valendo-se de auditorias, exigência de sistemas de compliance, reporte e mecanismos de revisão³³⁶. Em texto clássico, Braithwaite traz o conceito heterônimo de “*enforced self-regulation*”, pelo qual o Estado exige que empresas formulem regras internas e planos de conformidade, mas mantém poderes de supervisão e sanção para assegurar que tal autorregulação não se converta em mera retórica³³⁷.

Analizando-a diretamente no campo da proteção de dados pessoais, Bioni indica também a relação entre a metarregulação e o alocamento e mitigação de risco, reconhecendo que o modelo regulatório

se caracteriza como um processo em que autoridades estatais fiscalizam os processos de gerenciamento de riscos conduzidos pelos próprios atores regulados. Há, em parte, a delegação das tarefas regulatórias aos próprios agentes econômicos que estariam em melhores condições para mitigar os riscos das suas próprias atividades, e não somente o próprio Estado.³³⁸

Metarregulação, portanto, não implica desregulação. Ao contrário, pressupõe uma arquitetura normativa que define objetivos, princípios e deveres mínimos a serem cumpridos pelos agentes regulados, delegando-os a tarefa de construir mecanismos internos

336 GRABOSKY, Peter. Meta-regulation. In: DRAHOS, Peter (org.). *Regulatory theory: foundations and applications*. Canberra: ANU Press, 2017.

337 BRAITHWAITE, John. *Enforced self-regulation: a new strategy for corporate crime control*. Michigan Law Review, v. 80, n. 7, 1982, p. 1466-1507.

338 BIONI, Bruno Ricardo. Abrindo a “Caixa de Ferramentas” da LGPD para dar Vida ao Conceito ainda Elusivo de Privacy by Design. In: BIONI, Bruno. MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JUNIOR, Otavio Luiz. *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2021. p. 248.

aptos a conformar sua atividade à norma. Justamente por estes contornos, o arranjo metarregulatório tem sido utilizado em campos de elevada complexidade técnica e mutatividade acelerada, nos quais uma regra estanque tende a ficar rapidamente obsoleta ou a gerar incentivos perversos, como conformidades meramente formais e que não produzam real mitigação de riscos – dentre os quais a proteção de dados está situada.

Outro conceito útil para a compreensão da metarregulação, e que encontra respaldo nas iniciativas metarregulatórias presenciadas no ordenamento jurídico brasileiro, é o de regulação por princípios. Em vez de detalhar exaustivamente condutas permitidas e proibidas, o regulador estabelece princípios e resultados esperados, deixando espaço para que organizações ajustem meios e procedimentos às suas realidades. Julia Black identifica paradoxos dessa forma regulatória: por um lado, princípios permitem flexibilidade e adaptação; por outro, podem ampliar incerteza e abrir margem para interpretações estratégicas, exigindo do regulador capacidade de orientação e de *enforcement* para evitar a diluição dos padrões estabelecidos³³⁹.

Em um cenário de regulação por princípios, a metarregulação reforça a possibilidade de concretização destes. A exigência de avaliações de impacto, políticas de governança, registro de operações e canis de resposta a incidentes e atendimento de titulares, abordados adiante, refletem uma tentativa de conversão de princípios em procedimentos que o efetivem na prática.

A regulação torna-se policêntrica: além do Estado, associações setoriais, organismos de certificação, plataformas digitais e até padrões técnicos globais influenciam comportamentos. A metarregulação, nesse cenário, pode ser lida como tentativa de o Estado articular e supervisionar esse ecossistema, reconhecendo que parte relevante da governança ocorre dentro das organizações e por meio de padrões privados.

339 BLACK, Julia. *Forms and paradoxes of principles-based regulation*. LSE Law, Society and Economy Working Papers, n. 13/2008. London: London School of Economics, 2008.

Riscos e limitações da metarregulação.

Apesar de sua aparente conformidade com contextos de ausência de eficaz regulação estatal e necessidade de acompanhamento de uma realidade em contante transformação, a metarregulação não está ausente de riscos ou limitações.

Cita-se, a título exemplificativo, o risco de captura regulatória ou de colonização cognitiva, manifestado quando o regulador depende intensamente das informações e do *know-how* dos regulados. A informação compartilhada pelo agente regulado não corresponde, muitas vezes, à sua completa realidade, existindo sempre um viés de interesse do agente regulado em não compartilhar detalhes que potencialmente o prejudiquem, o que gera uma assimetria informacional intransponível. Além disso, a busca por informação pelo ente regulador é onerosa e não raro sofre pouca receptividade do regulado³⁴⁰.

Outro risco considerável é o da “performatividade” da conformidade, isto é, a criação de políticas e procedimentos que produzem aparência de conformidade, mas que não impactam de forma significativa em práticas decisórias. Conforme exposto, a efetividade da metarregulação pressupõe o efetivo envolvimento e disposição do agente regulado na utilização da caixa de ferramentas regulatória para uma gestão de risco mais informada e precisa; agindo o ente regulado meramente para cumprimento de deveres formais, o conteúdo da lógica metarregulatória esgota-se rapidamente. Em ambientes altamente burocratizados, a conformidade pode ser traduzida em documentos padronizados, checklists e relatórios que satisfazem formalidades, sem reduzir efetivamente riscos ou danos. Quando aplicada apenas como norma moralizante ou racionalizante, a metarregulação pode falhar em enfrentar dinâmicas reais de poder

340 PINTO JR, Helder Q; PIRES, Melissa Cristina Pinto. *Assimetria de Informações e Problemas Regulatórios*. Agência Nacional de Petróleo, 2000.

e de incentivos nas organizações, reproduzindo um abismo entre norma e prática³⁴¹.

Por fim, há o risco de desigualdade regulatória. Grandes organizações tendem a ter recursos para implementar programas sofisticados de compliance e governança, enquanto pequenos agentes enfrentam custos proporcionais mais elevados, o que pode gerar barreiras de entrada e concentração de mercado. Não obstante, agentes de pequeno porte – relevantes sobretudo em sociedades como a brasileira, marcadas por elevado grau de informalidade – sofrem também com barreiras informacionais, recrudescidas quando não há políticas públicas de conscientização e educação corporativa. Uma estratégia metarregulatória precisa, portanto, calibrar obrigações e oferecer instrumentos proporcionais, além de se alcançar agentes de pequeno porte, sob pena de se tornar inócua para parte relevante da sociedade.

2. METARREGULAÇÃO NO CONTEXTO DA ESTRATÉGIA DE REGULAÇÃO DA PROTEÇÃO DE DADOS PESSOAIS NO BRASIL.

2.1 A LGPD e o arcabouço regulatório da proteção de dados pessoais.

A LGPD compreende a sistematização do regime geral de proteção de dados pessoais baseado em princípios, direitos e deveres de agentes de tratamento. Ao lado de bases legais e hipóteses de tratamento de dados pessoais, o legislador estabeleceu deveres organizacionais, trazendo parâmetros e regras gerais de segurança, prevenção, responsabilização e prestação de contas. O princípio da *accountability*, em especial, assume feição metarregulatória, ao exigir não apenas conformidade, mas sua efetiva demonstração e publicização. Bioni caracteriza a *accountability* como eixo de uma “regulação e proteção

341 SIMON, F. C. *Meta-regulation in practice: beyond normative views of morality and rationality*. London: Routledge, 2017.

de dados pessoais” que desloca o foco para mecanismos internos de governança e transparência³⁴².

Bioni também defende que a LGPD representa uma “nova roupagem” da legislação em proteção de dados, em que o foco passa a ser a administração de riscos. A relação entre o direito e tecnologia, sob essa perspectiva, é resumida por Bioni no seguinte trecho:

Decompondo a palavra meta-regulação, metas são estabelecidas pela legislação que serão alcançadas colaborativamente por todos os agentes do ecossistema. Desta forma, os atores regulados têm discricionariedade para formular seus respectivos processos de gestão de riscos. Por outro lado, espera-se que tais processos sejam monitorados pelos órgãos reguladores e pelo restante da comunidade afetada por tais atividades econômicas.³⁴³

Refletindo o arranjo metarregulatório, a LGPD não prescreve previamente todas as medidas técnicas e administrativas adequadas a cada operação de tratamento de dados pessoais. Combina, pois, obrigações abertas – exemplificadamente, a adoção de medidas de segurança aptas a garantir a proteção dos dados – com expectativas de gestão de riscos e documentação, tais como registro de operações, comunicação de incidentes, relatórios de impacto em determinados cenários e atendimento a direitos dos titulares.

Esse arranjo favorece uma lógica de responsabilidade distribuída. Agentes de tratamento são compelidos a mapear atividades, justificar escolhas, demonstrar proporcionalidade e instituir controles. Ao mesmo tempo, os titulares e a sociedade ganham instrumentos de contestação e de exigência de transparência dos agentes. A ANPD, por sua vez, interpreta princípios, define parâmetros mínimos, fiscaliza e sanciona falhas, incentiva boas práticas e dialoga com a sociedade.

342 BIONI, Bruno. *Regulação e proteção de dados pessoais: o princípio da accountability*. Rio de Janeiro: Forense, 2022.

343 BIONI, Bruno Ricardo. *Abrindo a “Caixa de Ferramentas” da LGPD para dar Vida ao Conceito ainda Elusivo de Privacy by Design*. In: BIONI, Bruno. MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JUNIOR, Otavio Luiz. *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2021. p. 241.

Vale mencionar que aspectos metarregulatórios em matéria de proteção de dados pessoais não foram inaugurados somente com a LGPD; entretanto, foi com ela que assumiram sua forma mais completa, eficaz e coesa. Ainda que regre aspectos gerais do uso da internet no Brasil, o Marco Civil da Internet já trazia disposições atinentes a tratamento de dados pessoais no ambiente digital, sendo dotado de caráter fortemente principiológico. No entanto, conforme exposto em acertada crítica de Tomasevicius Filho³⁴⁴, a norma legal então promulgada pouco inovou na matéria, repetindo princípios entabulados na Constituição Federal sem precisas implicações práticas, tampouco consagrando uma estrutura regulatória que permitisse a atualização e refinamento das práticas abordadas na lei. Resultado disso foi uma lei que, embora dotada de elevado *pedigree* democrático, sendo sua elaboração marcada por consultas a diversos setores da sociedade, não conseguiu garantir a aplicabilidade de diversos princípios nela entabulados. A exemplo desta dificuldade em efetivação de deveres e padrões mínimos, citam-se as diversas posições conflitantes acerca da inconstitucionalidade do artigo 19 do Marco Civil³⁴⁵.

O recente histórico de experiências regulatórias relativamente similares é, portanto, indicativo da bem-sucedida estrutura trazida pela LGPD, que será examinada de forma mais aprofundada a seguir.

2.2 Instrumentos regulatórios da proteção de dados pessoais

A LGPD trouxe diversos instrumentos que refletem o conceito de metarregulação, trazendo contornos gerais de expectativa de

344 TOMASEVICIUS FILHO, Eduardo. *Marco Civil da Internet: uma lei sem conteúdo normativo*. Estudos Avançados v. 30. Faculdade de Direito da Universidade de São Paulo, p. 269-285, 2016.

345 SUPREMO TRIBUNAL FEDERAL (STF). *STF define parâmetros para responsabilização de plataformas por conteúdos de terceiros*. Notícias STF, 26 jun. 2025. Disponível em: <https://noticias.stf.jus.br/postsnoticias/stf-define-parametros-para-responsabilizacao-de-plataformas-por-conteudos-de-terceiros/>. Acesso em: 4 fev. 2026

elaboração de normas e procedimentos (artigo 50, § 2º, inciso I), adoção de padrões e boas práticas (artigos 12, § 3º, 32, 40, 46, § 1º, 49, 51 e 55-J, inciso VIII), estímulo a adoção de códigos de conduta e certificação por agentes de tratamento (artigos 33, inciso II, “d” e 50, § 2º, inciso II) e produção de orientações para agentes de tratamento (artigo 55-J, inciso XVIII). A redação dos dispositivos mencionados tem textura aberta, a ser complementada por regulamentações e atos da ANPD, o que cumpre o papel de permitir a inovação e a adaptabilidade das normas a contextos cambiantes ao mesmo tempo em que se assegura a necessidade de observância e adoção de um padrão mínimo ou a legítima expectativa de que os agentes de tratamento o façam.

Dentre os instrumentos mencionados, os códigos de conduta e certificação representam uma estrutura consolidada internacionalmente, traduzindo princípios da LGPD em requisitos verificáveis e afirmando o valor de determinadas estruturas de governança, como alocação de atribuições, consolidação de procedimentos de avaliação de risco, gestão de incidentes e atendimento ao titular e mensuração de sua efetividade³⁴⁶. Além disso, a validação coletiva de códigos de conduta e certificação geram um incentivo positivo para os agentes de tratamento que o incorporarem em suas atividades, servindo de sinal distintivo do nível de conformidade da empresa e impulsionando contratos e iniciativas com terceiros, facilitando relações com o poder público e melhorando sua imagem perante o mercado consumidor em geral.

Entretanto, a eficácia desses instrumentos depende de dois fatores centrais: credibilidade e executoriedade. Padrões precisam ser substantivos e auditáveis; caso contrário, correm o risco de serem reduzidos a enunciados propagandísticos. Ademais, sem ameaça real de fiscalização e sanção, códigos e certificações podem se transformar em mecanismos de legitimação simbólica. Nesse sentido, a mera exposição dos instrumentos na LGPD não basta para sua aplicabilidade, sendo necessária a constante avaliação e validação dos instrumentos

346 JONES, Joe; FISCHER, Luke; SANIUK-HEINIG, Cheryl; KANTHASAMY, Saz. *Privacy Governance Report 2024*. Portsmouth, NH: IAPP, 2024.

adotados pelos agentes, para que estes sejam incentivados, e a capacidade de efetiva intervenção quando os mecanismos falham ou são utilizados de forma oportunista³⁴⁷.

A título exemplificativo, cumpre mencionar a ausência de aprovação de cláusulas contratuais equivalente e específicas e de normas corporativas globais de transferência internacional de dados pela ANPD³⁴⁸. Embora a agência tenha com sucesso aprovado o Regulamento de Transferência Internacional de Dados e o conteúdo das cláusulas-padrão contratuais – Resolução CD/ANPD nº 19, de 23 de agosto de 2024³⁴⁹ – e declarado a União Europeia organismo internacional adequado para transferência internacional de dados – Resolução nº 32, de 26 de janeiro de 2026³⁵⁰ –, a não aprovação de referidos instrumentos gera incertezas e, em última análise, resulta em procedimentos de transferência internacional de dados que não adotem as hipóteses legais já existentes. A ausência de complementação da regulação já existente é, pois, condição *sine qua non* para que os instrumentos previstos na LGPD e iniciados pela atuação recente da ANPD sejam concretizados plenamente.

Em matéria diversa, a ANPD disciplinou com sucesso a diferenciação do regime aplicável a agentes de pequeno porte, calibrando deveres e expectativas das operações de tratamento

347 BRAITHWAITE, John. *Enforced self-regulation: a new strategy for corporate crime control*. Michigan Law Review, v. 80, n. 7, 1982, p. 1466-1507.

348 BRASIL. Agência Nacional de Proteção de Dados (ANPD). *Transferência internacional de dados*. [s.d.]. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/assuntos-internacionais/transferencia-internacional-de-dados>. Acesso em: 13 fev. 2026.

349 BRASIL. Agência Nacional de Proteção de Dados. Conselho Diretor. *Resolução CD/ANPD nº 19, de 23 de agosto de 2024*. Aprova o Regulamento de Transferência Internacional de Dados e o conteúdo das cláusulas-padrão contratuais. *Diário Oficial da União*: Brasília, DF, 23 ago. 2024. Seção 1, p. 123-127. Disponível em: <https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-19-de-23-de-agosto-de-2024-580095396>. Acesso em: 13 fev. 2026.

350 BRASIL. Agência Nacional de Proteção de Dados. *Resolução nº 32, de 26 de janeiro de 2026*. Dispõe sobre o reconhecimento da União Europeia como organismo internacional com grau de proteção de dados pessoais adequado ao previsto na Lei nº 13.709, de 14 de agosto de 2018, para fins de transferência internacional de dados. *Diário Oficial da União*: Brasília, DF, 27 jan. 2026. Seção 1, p. 49. Disponível em: <https://www.in.gov.br/web/dou/-/resolucao-n-32-de-26-de-janeiro-de-2026-683334547>. Acesso em: 13 fev. 2026.

à capacidade de conformidade destes. A Resolução CD/ANPD nº 2/2022³⁵¹ acertadamente flexibiliza certas obrigações e prevê modelos simplificados, buscando compatibilizar custos de conformidade e proteção efetiva, sem afastar a possibilidade de exigências mais rigorosas conforme o risco do tratamento.

3. O PAPEL DA ANPD NA ESTRATÉGIA REGULATÓRIA DE PROTEÇÃO DE DADOS PESSOAIS.

3.1 Desenho institucional e competências.

A ANPD foi instituída como órgão da administração pública federal responsável por zelar, implementar e fiscalizar a LGPD, com competências normativas, fiscalizatórias e sancionadoras. Seu desenho institucional foi disciplinado inicialmente pelo Decreto nº 10.474/2020, que estruturou Conselho Diretor e órgãos internos, além de prever mecanismos de participação social por meio do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade.

Após anos de incerteza e alterações diversas em sua natureza, a ANPD finalmente tornou-se agência junto à criação do chamado “ECA Digital”³⁵², solidificando um movimento iniciado por parte da doutrina^{353 354}, que, assim como a sociedade civil, chamava atenção

351 BRASIL. Agência Nacional de Proteção de Dados. *ANPD lança Painel da Fiscalização*. Brasília, 12 nov. 2025. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-lanca-painel-da-fiscalizacao>. Acesso em: 13 fev. 2026.

352 MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS (MGI). *Governo sanciona ECA Digital e anuncia transformação da ANPD em agência reguladora*. Notícias, 18 set. 2025. Disponível em: <https://www.gov.br/gestao/pt-br/assuntos/noticias/2025/se/governo-sanciona-eca-digital-e-anuncia-transformacao-da-anpd-em-agencia-reguladora>. Acesso em: 15 fev. 2026.

353 DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006. p. 388.

354 DE LIMA, Cíntia Rosa Pereira. *Autoridade nacional de proteção de dados e a efetividade da Lei Geral de Proteção de Dados (Lei n. 13.709/2018 e as alterações da Lei n. 13.853/2019), o Marco Civil da Internet (Lei n. 12.965/2014) e as sugestões de alteração do CDC (PL 3.514/2015)*. São Paulo: Almeida, 2020.

para a imprescindibilidade de uma autoridade nacional de proteção de dados forte e independente.

Do ponto de vista metarregulatório, a agência desempenha funções de arquitetura e de coordenação, na medida em que (i) produz interpretações oficiais e orientações capazes de estabilizar expectativas do titular de dados e do agente de tratamento; (ii) define critérios para procedimentos de fiscalização; (iii) exerce poder sancionador e celebra instrumentos de adequação com agentes de tratamento infratores; e (iv) coordena referenciais de conformidade.

4. AGENDA REGULATÓRIA E PRIORIZAÇÃO DE TEMAS.

O referencial mais importante para compreensão da atuação da ANPD no arranjo metarregulatório compreende sua agenda regulatória. Por meio dela, constata-se a priorização de temas e a capacidade de alocação de recursos para direcioná-los. A existência de agenda regulatória cria previsibilidade e permite aferir publicamente a efetividade do papel regulador da ANPD. Além disso, funcionam como instrumento de metarregulação indireta, sinalizando aos agentes regulados quais temas serão escrutinados e gerando expectativas de adequação e dedicação orçamentária a matérias específicas em proteção de dados. Trata-se, além de mera listagem de iniciativas do poder público, de mecanismo que traz sinergia entre regulador e regulado, conforme reconhecido pela doutrina³⁵⁵.

Em dezembro de 2025, a ANPD divulgou atualização de sua Agenda Regulatória 2025-2026³⁵⁶ e publicou mapa de temas prioritários para o biênio 2026-2027, com inclusão de novos tópicos associados à

355 PARENTONI, Leonardo Netto. *Por que confiar na Autoridade Nacional de Proteção de Dados?* Revista da Faculdade de Direito da UFMG: Belo Horizonte, n. 79, pp. 163-192, jul./dez.2021, p. 182.

356 BRASIL. Agência Nacional de Proteção de Dados. Conselho Diretor. *Resolução CD/ANPD nº 31, de 22 de dezembro de 2025*. Altera a Agenda Regulatória para o biênio 2025-2026. *Diário Oficial da União*: Brasília, DF, 24 dez. 2025. Seção 1, p. 858-860. Disponível em: <https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-31-de-22-de-dezembro-de-2025-677950080>. Acesso em: 15 fev. 2026.

implementação do chamado “ECA Digital”, indicando expansão do escopo regulatório e revisões futuras de regras de fiscalização e sanção.

A análise comparativa da agenda regulatória atual com as agendas regulatórias anteriores permite ter noção mais precisa acerca da (in)eficácia de regulamentação de matérias diversas pela agência:

Tabela 1 – Análise não exaustiva de temas da agenda regulatória da ANPD

Tema	Realizado?	Ato	Ano de início planejado	Ano de entrega
Agentes de pequeno porte	Sim	Res. CD/ANPD nº 2	2022	2022
Sanções	Sim	Res. CD/ANPD nº 4	2022	2023
Direitos dos titulares	Não	n/a	2023	n/a
Incidentes de segurança	Sim	Res. CD/ANPD nº 15	2022	2024
RIPD	Não	n/a	2022	n/a
Encarregado	Sim	Res. CD/ANPD nº 18	2022	2024
Transferência internacional	Sim	Res. CD/ANPD nº 19	2022	2024
Hipóteses de tratamento	Parcialmente	Guia Orientativo – Legítimo Interesse	2023	2024
Dados sensíveis	Não	n/a	2022	n/a
Tratamento acadêmico	Sim	Guia Orientativo	2022	2023
Anonimização	Parcialmente	Estudo Técnico	2022	2023
Compartilhamento pelo poder público	Não	n/a	2024	n/a
Dados de criança e adolescente	Não	n/a	2024	n/a

Tema	Realizado?	Ato	Ano de início planejado	Ano de entrega
Medidas de segurança	Não	n/a	2024	n/a
Inteligência artificial	Não	n/a	2024	n/a
Boas práticas e governança	Não	n/a	2024	n/a
Agregadores de dados pessoais	Não	n/a	2026	n/a

Nota-se que a ANPD tem, majoritariamente, adotado uma agenda regulatória bem-sucedida, com a maior parte dos temas tendo sido regulamentados dentro de um a dois anos do início do procedimento regulatório.

No entanto, ainda não foi apresentada regulamentação atinente a pontos de elevada importância, como o exercício de direitos dos titulares, dados sensíveis, o compartilhamento de dados pelo poder público, medidas de segurança, dados de criança e adolescente e elaboração do relatório de impacto em proteção de dados (RIPD), o que diminui a eficácia da norma em relação a tópicos relevantes. Tome-se, como exemplo, a elaboração do RIPD; visto que a LGPD recomenda que seja realizada antes do início do tratamento dos dados pessoais, deveria tal disposição legal ter sido acompanhada de uma regulamentação que trouxesse contornos mais precisos a este relatório e garantisse, assim, maior segurança jurídica aos agentes de tratamento e maior proteção ao titular de dados.

Não incluídos na agenda regulatória, igualmente relevantes são os radares tecnológicos elaborados pela ANPD, que refletem posicionamentos da agência acerca de temas emergentes, tendo sido abordados até o momento os seguintes temas: cidades inteligentes, biometria e reconhecimento facial, inteligência artificial generativa, neurotecnologias e métodos de aferição de idade digital. Ainda que não dotados da mesma força normativa, os radares tecnológicos cumprem as funções de integração entre regulador e regulado acima mencionadas.

5. FISCALIZAÇÃO, SANÇÕES E RACIONALIDADE RESPONSIVA.

Uma das primeiras publicações realizadas pela ANPD consiste no Regulamento do Processo de Fiscalização e do Processo Administrativo

Sancionador – Resolução CD/ANPD nº 1/2021³⁵⁷. No regulamento estabelecem-se fases e instrumentos do ciclo fiscalizatório, como monitoramento, orientação, prevenção e repressão, além de procedimentos formais do processo sancionador.

Posteriormente, a Resolução CD/ANPD nº 4/2023 aprovou o Regulamento de Dosimetria e Aplicação de Sanções Administrativas, definindo critérios para cálculo de multas e parâmetros de agravantes e atenuantes.

A atuação da ANPD tem, com razão, estabelecido sequencialmente critérios seguros de instauração e condução do procedimento fiscalizatório e sancionador, bem como dosimetria que garanta uma aplicação justa e proporcional de sanções, refletindo de forma adequada o arranjo metarregulatório.

No entanto, até o momento, a agência tem produzido número escasso de decisões – sobretudo envolvendo o setor privado. Ainda que não se ignore que a atuação do ente regulador deva se pautar primariamente nos aspectos orientador e fiscalizador, a ausência de punibilidade expressiva reduz a efetividade da regulamentação; além disso, uma jurisprudência administrativa mais robusta assegura maior segurança jurídica aos próprios agentes regulados.

6. CRÍTICA DA EFETIVIDADE DA ATUAÇÃO DA ANPD SOB PRISMA METARREGULATÓRIO.

6.1 Capacidade institucional, recursos e coerência regulatória.

A efetividade de um modelo regulatório baseado na metarregulação se apoia, em considerável proporção, na capacidade

357 BRASIL. Agência Nacional de Proteção de Dados. Conselho Diretor. *Resolução CD/ANPD nº 1, de 28 de outubro de 2021*. Aprova o Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dados. Diário Oficial da União: Brasília, DF, 29 out. 2021. Edição 205, Seção 1, p. 6. Disponível em: <https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-1-de-28-de-outubro-de-2021-355817513>. Acesso em: 20 fev. 2026.

avaliativa do ente regulador. A fiscalização de instrumentos de governança e *accountability* pressupões a capacidade do regulador de avaliar a qualidade das ferramentas adotadas pelo regulado e de assertivamente indicar falhas, lacunas e imprecisões que indiquem não-conformidade da solução com o que se exige segundo o estado da técnica.

A demonstração do mais alto nível de *expertise* técnica nas questões diversas que envolvam tratamento de dados pessoais, especialmente as que envolvam a compreensão de arquiteturas técnicas, fluxos de dados, decisões algorítmicas, práticas de segurança da informação, entre outros, implica na imprescindibilidade de que a ANPD seja composta de um corpo técnico altamente especializado. Manifestações públicas da agência acerca da necessidade de investimentos³⁵⁸ apenas reforçam o que a doutrina já constataria no momento da estruturação da autoridade: a necessidade de investimentos expressivos para que o órgão tenha a efetividade pretendida³⁵⁹.

Conforme reconhecido por Parentoni, a ANPD amadureceu institucionalmente em período curto logo após sua fundação, “trazendo importantes sinalizações aos agentes de tratamento e aos titulares de dados pessoais, especialmente com relação a pontos nos quais a LGPD é dúbia ou omissa, deliberadamente delegando à autoridade nacional a definição de padrões e o preenchimento de lacunas”³⁶⁰. No entanto, conforme passa a regulamentar temas diversos – sendo inclusive provável agente regulador da inteligência artificial no Brasil³⁶¹ –, passa

358 BRACCO, Matheus. *Presidente da ANPD pede por mais investimentos no Congresso Nacional*. Security Leaders, 20 out. 2023. Disponível em: <https://securityleaders.com.br/presidente-da-anpd-pede-por-mais-investimentos-no-congresso-nacional/>. Acesso em: 20 fev. 2026.

359 DE LIMA, Cíntia Rosa Pereira. *Autoridade nacional de proteção de dados e a efetividade da Lei Geral de Proteção de Dados (Lei n. 13.709/2018 e as alterações da Lei n. 13.853/2019), o Marco Civil da Internet (Lei n. 12.965/2014) e as sugestões de alteração do CDC (PL 3.514/2015)*. São Paulo: Almeida, 2020, p. 315.

360 PARENTONI, Leonardo Netto. *Por que confiar na Autoridade Nacional de Proteção de Dados?* Revista da Faculdade de Direito da UFMG: Belo Horizonte, n. 79, pp. 163-192, jul./dez.2021, p. 186.

361 SENADO aprova regulamentação da inteligência artificial: texto vai à Câmara. Distrito Federal, Agência Senado, 10 de dezembro de 2024. Disponível em: <https://www12.senado.gov.br/comunicacao/comunicacao.asp?id=1789>.

a ANPD a ter um desafio maior de garantir a coerência entre suas diferentes regulações.

A coerência deve se traduzir também no estabelecimento claro de prioridades e métricas. Conforme analisado, a ausência de análise crítica e objetiva de temas, acontecimentos e tendências gera o risco de que os princípios trazidos pela lei se esgotem na prática. Assim como os entes regulados, o regulador deve ter um planejamento estratégico consolidado e constantemente atualizado – mérito já logrado pela ANPD³⁶².

A estrutura de *reporting* periódico estabelecida pela elaboração e atualização das agendas regulatórias também contribui para esta finalidade, elencando de forma objetiva as prioridades no futuro próximo e médio da agência. Além disso, a publicação dos já mencionados radares tecnológicos traz maior segurança jurídica a partir da exposição do posicionamento do regulador acerca de temas de relevância e que possam ser objeto de regulamentação futura.

No entanto, é certo que medidas de publicidade e transparência como estas devam ser acompanhadas de evidência de impacto das iniciativas, relacionando-as a resultados observáveis, como redução de incidentes recorrentes, aumento de conformidade em setores críticos ou melhoria na experiência dos titulares ao exercer direitos.

7. LACUNAS E EFEITOS DO PROCESSO DE METARREGULAÇÃO.

Conforme analisado ao início deste trabalho, a metarregulação é composta de três momentos distintos de atuação do entre regulador, qual sejam, a orientação da sociedade, a fiscalização dos regulados e a punição de eventuais infratores.

senado.leg.br/noticias/materias/2024/12/10/senado-aprova-regulamentacao-da-inteligencia-artificial-texto-vai-a-camara. Acesso em: 13 de março de 2025.

362 BRASIL. Agência Nacional de Proteção de Dados (ANPD). *Planejamento Estratégico ANPD 2024-2027*. 7 maio 2024. Disponível em: <https://www.gov.br/anpd/pt-br/acesso-a-informacao/acoes-e-programas/governanca/governanca-estrategica/planejamento-estrategico/planejamento-estrategico-2024-2027>. Acesso em: 20 fev. 2026.

A fase de orientação tem sido cumprida pela ANPD através de instrumentos de *soft law* (notas técnicas, guias, recomendações) e mecanismos de participação (tomadas de subsídios, consultas, *sandbox* regulatório). Apesar de demandarem investimento adicional, conforme analisado acima, esta etapa é primordial para amadurecimento de regulador e regulado acerca de critérios e padrões gerais de conformidade, sobretudo no contexto de tecnologias emergentes e pouco conhecidas.

Contudo, a eficácia dessa etapa não prescinde de uma robusta fiscalização e sanção. Se a orientação não for seguida por monitoramento e por intervenções seletivas, há risco de que agentes oportunistas se beneficiem do baixo custo de descumprir a norma, deslocando o ônus para titulares e para o sistema de justiça.

O já mencionado regulamento de fiscalização prevê uma lógica escalonada, com etapas de monitoramento, orientação e prevenção, além de procedimento sancionador pré-estabelecido. Embora esta estrutura seja, *a priori*, compatível com a executoriedade responsiva, a frequência e quantidade de procedimentos fiscalizatórios em curso e a publicidade de seus efeitos e aprendizados – não dos procedimentos em si, ressalte-se – compõem parte crucial do aferimento da efetividade de atuação do ente regulador. A fiscalização de empresas relevantes por ausência de canal adequado de comunicação com encarregado³⁶³ escancara como temas indispensáveis e básicos de tratamento de dados podem acabar negligenciados caso o poder público não os fiscalize de forma constante.

Ao detalhar os critérios de dosimetria das sanções, a Resolução CD/ANPD nº 4/2023 contribui para previsibilidade dos riscos administrativos a que estão sujeitos os agentes de tratamento. Porém, também expõe a necessidade de que a agência desenvolva jurisprudência administrativa consistente. Em áreas novas, decisões

363 BRASIL. Agência Nacional de Proteção de Dados (ANPD). *ANPD fiscaliza 20 empresas por falta de Encarregado e canal de comunicação adequado*. 13 dez. 2024. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-fiscaliza-20-empresas-por-falta-de-encarregado-e-canal-de-comunicacao>. Acesso em: 22 fev. 2026.

contraditórias ou excessivamente casuísticas podem enfraquecer incentivos para investimento em governança e estimular litigância estratégica. Uma jurisprudência estável – com fundamentação técnica e jurídica robusta – tende a reduzir custos de conformidade e a fortalecer a dimensão pedagógica das sanções.

Outro ponto de risco mencionado ao longo deste trabalho é a conformidade meramente formalística, isto é, a produção de políticas, códigos e relatórios meramente formais, que não afetem procedimentos internos ou impactem na tomada de decisões que envolvam o tratamento de dados pessoais. A fiscalização deve envolver uma análise completa de pontos relevantes, como se avaliações de impacto são utilizadas antes de operações de risco, se há efetiva participação do encarregado em projetos e diálogo significativo deste com o órgão interno de governança em proteção de dados, se os incidentes são mitigados e reportados de forma eficiente, organizada e tempestividade, se há auditoria padronizada de terceiros na cadeia de fornecimento...

A regulamentação da comunicação de incidentes de segurança é importante mecanismo de fiscalização criado pela ANPD³⁶⁴ e que serve de referencial para a política regulatória em temas futuros. Ao definir critérios e prazos de comunicação, a agência reduz margem para subnotificação estratégica e introduz um critério de avaliação das condutas dos agentes regulados. Porém, a efetividade real do instrumento regulatório dependerá da análise periódica da capacidade de análise das comunicações recebidas, análise de padrões e seleção de casos exemplares para revisão crítica e possível reestruturação futura. Ademais, a regra de notificação geral de todos os titulares envolvidos no incidente tem sido parcialmente contestada sob o argumento de que aumentaria o risco de subnotificação em razão do elevado custo

364 BRASIL. Agência Nacional de Proteção de Dados (ANPD). *ANPD aprova o Regulamento de Comunicação de Incidente de Segurança*. 26 abr. 2024. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-aprova-o-regulamento-de-comunicacao-de-incidente-de-seguranca>. Acesso em: 22 fev. 2026.

operacional e reputacional³⁶⁵, o que reflete a importância de periódica reavaliação e potencial alteração da norma.

8. LIMITES ESTRUTURAIS E ECONOMIA POLÍTICA.

Conforme analisado, a afetividade da metarregulação é impactada por fatores como a limitação de recursos e investimento, a coerência organizativa e regulatória do agente regulador e a necessidade de harmonização dos aspectos orientador, fiscalizador e sancionador da regulação responsiva. Tratam-se, todos, de elementos relacionados a capacidades internas do agente regulador.

No entanto, a regulação eficiente está condicionada também a fatores externos. Um fator já mencionado no início deste trabalho consiste na assimetria de informação entre regulador e regulado. Esta assimetria também se dá sob o aspecto econômico: empresas de grande porte, sejam *big techs* ou multinacionais consolidadas em setores tradicionais, têm alto poder de *lobby*, recursos de litigância estratégica em massa e capacidade de intervenção e influência na esfera pública.

Outro fator relevante é a multipolaridade de entidades regulatórias. A LGPD deixa claro que a ANPD não é órgão único de regulação da matéria de proteção de dados pessoais, de modo que sua atividade regulatória coexiste com instituições como o Procon, a Secretaria Nacional do Consumidor (Senacon), o Banco Central do Brasil, a Comissão de Valores Mobiliários, entre outros. Se por um lado a descentralização da atividade regulatória possa propiciar uma regulação mais efetiva – na medida em que cada instituição tem o mais elevado grau de *expertise* em seu próprio setor –, por outro, corre-se o risco de sobreposições ou lacunas normativas, bem como de conflitos de agenda e interesses entre os órgãos. Cabe à ANPD, portanto, assumir o papel de condução de parcerias que propiciem um desenvolvimento

365 DATA PRIVACY BRASIL. *Contribuição Data Privacy Brasil – Regulamento de Comunicação de Incidente de Segurança com Dados Pessoais*.

harmônico e integrado da regulação da proteção de dados pessoais. Nesse sentido, a realização de publicações conjuntas entre diferentes órgãos favorece a executoriedade da regulação ao dar maior “peso” à medida, como observada na recente recomendação conjunta expedida pela ANPD, pelo Ministério Público Federal e pela Senacon à X Brasil, no contexto geração de conteúdos sexualizados pela ferramenta de inteligência artificial Grok³⁶⁶.

Um terceiro fator é a cultura organizacional de compliance. Em mercados onde a conformidade é percebida como custo e não como componente de qualidade e confiança, a tendência é de mínima adequação. A metarregulação busca alterar essa cultura ao tornar a governança verificável e sancionável; porém, sem casos paradigmáticos e consequências proporcionais, o incentivo dominante pode permanecer o de adequação ao mínimo necessário.

Por fim, há o desafio de riscos sistêmicos. Práticas de coleta massiva e perfilamento podem gerar danos difusos (por exemplo, discriminação algorítmica ou manipulação comportamental) que não são facilmente capturados por reclamações individuais ou por inspeções pontuais. Uma agência focada em processos de conformidade organizacional precisa desenvolver ferramentas para enxergar e atacar padrões setoriais, o que exige dados, capacidade analítica e priorização estratégica.

9. PARÂMETROS PARA APRIMORAMENTO.

À luz dos limites assinalados, é possível delinear parâmetros de aprimoramento de uma estratégia metarregulatória em proteção de dados.

366 BRASIL. Agência Nacional de Proteção de Dados (ANPD). *ANPD, MPF e Senacon recomendam que X impeça geração e circulação de conteúdos sexualizados indevidos por meio do Grok*. 20 jan. 2026. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-mpf-e-senacon-recomendam-que-x-impeca-geracao-e-circulacao-de-conteudos-sexualizados-indevidos-por-meio-do-grok>. Acesso em: 22 fev. 2026.

O primeiro parâmetro de aprimoramento compreende fortalecer a responsividade, agregando à orientação maior frequência e expressividade de intervenções e sancionamento em casos paradigmáticos. A maior relevância desta medida está na publicização da decisão e no caráter pedagógico que não se limita ao agente infrator, atingindo a coletividade, na medida em que fortalece a noção de executoriedade da regulação e dá contornos mais precisos aos direitos tutelados, favorecendo uma definição de risco mais eficaz pelos agentes regulados.

O segundo parâmetro compreende o desenvolvimento de modelos mais sistêmicos de governança baseada em risco e evidências. Com o aumento progressivo no número de temas regulados pela ANPD, e com o crescente conhecimento acumulado pela agência, avulta-se a importância de elaboração de guias ou *frameworks* gerais (ou setoriais) de proteção de dados, que possam ser adotados pelos agentes de tratamento e que tratem de forma compreensiva e sistêmica a atividade de tratamento, incluindo métricas e modelos de avaliação interna.

O terceiro parâmetro consiste na manutenção de diálogo interativo entre regulador e regulado. Embora interações frequentes com empresas de grande porte sejam mais costumeiras, o contato com agentes informais e de pequeno porte tende a naturalmente se encaminhar para um esgotamento, razão pela qual se deve manter uma política constante de educação e conscientização, adentrando a ANPD em centros de formação e entidades cívicas e setoriais, garantindo que a conformidade seja efetivada até no menor grau de atuação.

O quarto e último parâmetro envolve a institucionalização da cooperação policêntrica. A metarregulação funciona melhor quando o regulador estatal consegue orquestrar o ecossistema regulatório; acordos de cooperação com autoridades setoriais, integração com políticas de segurança cibernética, e coordenação com órgãos de defesa do consumidor e do Ministério Público representam algumas das medidas que fortalecem uma cultura coesa de proteção de dados pessoais e reduzem distorções entre setores diversos da sociedade.

CONSIDERAÇÕES FINAIS

A metarregulação, conceituada como estratégia de coordenação e regulação da autorregulação por meio de uma agência reguladora estatal, mostra-se adequada à regulação da proteção de dados pessoais, em razão da elevada complexidade técnica e mutabilidade acelerada das tecnologias e atividades que envolvam o tratamento de dados pessoais. Nesse contexto, a LGPD opta por um desenho regulatório predominantemente principiológico e orientado à gestão de riscos, priorizando critérios e parâmetros de estruturação de arranjos de governança, *accountability* e demonstração de conformidade.

A ANPD, como parte fundamental este arranjo metarregulatório, exerce função de coordenação de parâmetros mínimos, orientação de agentes de tratamento, definição de conceitos basilares e afirmação de executoriedade. Em seu histórico, a agência tem acumulado méritos relevantes, cumprindo satisfatoriamente o papel de orientação a partir da complementação da textura aberta da LGPD e da publicidade de seu planejamento e atuação, bem como de indicação de movimentos regulatórios. Esta atuação tem sido fundamental para o fortalecimento de segurança jurídica em matéria de proteção de dados e para a efetivação de comandos legais. Por outro lado, a agenda regulatória tem se demonstrado insuficiente para a regulamentação célere e efetiva de temas de elevada importância, como tratamento de dados sensíveis e de crianças e adolescentes, direitos de titulares e elaboração de relatórios de impacto.

Somam-se a estas deficiências limitações inerentes ao arranjo metarregulatório. A limitação de recursos, sobretudo financeiros, implica na inviabilidade de atuação especializada em todas as frentes de forma simultânea, o que interfere na necessidade de priorização de temas em detrimento de outros, e na paridade da relação entre regulador e regulado. De forma complementar, a escassez de decisões públicas em processos administrativos enfraquece o poder executório da agência, ao mesmo tempo em que mantém incertezas que poderiam ser sanadas ou diminuídas por meio da consolidação de uma

jurisprudência administrativa expressiva. Ademais, existem desafios econômicos e políticos inevitáveis, tais como assimetrias econômicas e de informação, concentração de mercado, capacidade de litigância e pressões por flexibilização, além da necessidade de coordenação policêntrica com outras autoridades e órgãos com competências correlatas.

Em síntese, o trabalho sustenta que a metarregulação é uma parte essencial para compreensão da estratégia brasileira de regulação da proteção de dados pessoais, devendo ser analisada a partir de sua principal manifestação: a ANPD. A estratégia metarregulatória tem demonstrado, em pouco tempo, resultados satisfatórios; entretanto, o reconhecimento da ineficiência da regulação em determinadas matérias e a existência de limites próprios da estratégia regulatória devem ser levados em consideração para compreensão real de pontos de correção e melhora oportunos. Para isso, torna-se fundamental (i) intensificar as fases mais deficitárias do ciclo de regulação responsiva adotado pela agência; (ii) produzir modelos sistêmicos de governança baseados em riscos e evidências; e (iii) manter diálogo sustentável e permanente com os diferentes setores da sociedade; e (iv) garantir uma cooperação policêntrica entre os diferentes agentes reguladores.

São esses, em última instância, os desafios que definirão se o arranjo metarregulatório da LGPD tornará a proteção de dados um padrão real de governança.

REFERÊNCIAS

BIONI, Bruno Ricardo. *Abrindo a “Caixa de Ferramentas” da LGPD para dar Vida ao Conceito ainda Elusivo de Privacy by Design*. In: BIONI, Bruno. MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JUNIOR, Otavio Luiz. *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2021.

BIONI, Bruno. *Regulação e proteção de dados pessoais: o princípio da accountability*. Rio de Janeiro: Forense, 2022.

BLACK, Julia. *Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a ‘Post-Regulatory’ World*. *Current Legal Problems* v. 54, p. 105, 2001.

BLACK, Julia. *Forms and paradoxes of principles-based regulation*. LSE Law, Society and Economy Working Papers, n. 13/2008. London: London School of Economics, 2008.

BRACCO, Matheus. Presidente da ANPD pede por mais investimentos no Congresso Nacional. *Security Leaders*, 20 out. 2023. Disponível em: <https://securityleaders.com.br/presidente-da-anpd-pede-por-mais-investimentos-no-congresso-nacional/>. Acesso em: 20 fev. 2026.

BRAITHWAITE, John. *Enforced self-regulation: a new strategy for corporate crime control*. *Michigan Law Review*, v. 80, n. 7, 1982, p. 1466-1507.

BRASIL. Agência Nacional de Proteção de Dados (ANPD). *Transferência internacional de dados*. [s.d.]. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/assuntos-internacionais/transferencia-internacional-de-dados>. Acesso em: 13 fev. 2026.

BRASIL. Agência Nacional de Proteção de Dados. Conselho Diretor. *Resolução CD/ANPD nº 19, de 23 de agosto de 2024. Aprova o Regulamento*

de Transferência Internacional de Dados e o conteúdo das cláusulas-padrão contratuais. Diário Oficial da União: Brasília, DF, 23 ago. 2024. Seção 1, p. 123-127. Disponível em: <https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-19-de-23-de-agosto-de-2024-580095396>. Acesso em: 13 fev. 2026.

BRASIL. Agência Nacional de Proteção de Dados. Resolução nº 32, de 26 de janeiro de 2026. *Dispõe sobre o reconhecimento da União Europeia como organismo internacional com grau de proteção de dados pessoais adequado ao previsto na Lei nº 13.709, de 14 de agosto de 2018, para fins de transferência internacional de dados.* Diário Oficial da União: Brasília, DF, 27 jan. 2026. Seção 1, p. 49. Disponível em: <https://www.in.gov.br/web/dou/-/resolucao-n-32-de-26-de-janeiro-de-2026-683334547>. Acesso em: 13 fev. 2026.

BRASIL. Agência Nacional de Proteção de Dados. ANPD lança Painel da Fiscalização. Brasília, 12 nov. 2025. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-lanca-painel-da-fiscalizacao>. Acesso em: 13 fev. 2026.

BRASIL. Agência Nacional de Proteção de Dados. Conselho Diretor. Resolução CD/ANPD nº 31, de 22 de dezembro de 2025. *Altera a Agenda Regulatória para o biênio 2025-2026.* Diário Oficial da União: Brasília, DF, 24 dez. 2025. Seção 1, p. 858-860. Disponível em: <https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-31-de-22-de-dezembro-de-2025-677950080>. Acesso em: 15 fev. 2026.

BRASIL. Agência Nacional de Proteção de Dados. Conselho Diretor. Resolução CD/ANPD nº 1, de 28 de outubro de 2021. *Aprova o Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dados.* Diário Oficial da União: Brasília, DF, 29 out. 2021. Edição 205, Seção 1, p. 6. Disponível em: <https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-1-de-28-de-outubro-de-2021-355817513>. Acesso em: 20 fev. 2026.

BRASIL. Agência Nacional de Proteção de Dados (ANPD). *Planejamento Estratégico ANPD 2024-2027*. 7 maio 2024. Disponível em: <https://www.gov.br/anpd/pt-br/acesso-a-informacao/acoes-e-programas/governanca/governanca-estrategica/planejamento-estrategico/planejamento-estrategico-2024-2027>. Acesso em: 20 fev. 2026.

BRASIL. Agência Nacional de Proteção de Dados (ANPD). *ANPD fiscaliza 20 empresas por falta de Encarregado e canal de comunicação adequado*. 13 dez. 2024. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-fiscaliza-20-empresas-por-falta-de-encarregado-e-canal-de-comunicacao>. Acesso em: 22 fev. 2026.

BRASIL. Agência Nacional de Proteção de Dados (ANPD). *ANPD aprova o Regulamento de Comunicação de Incidente de Segurança*. 26 abr. 2024. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-aprova-o-regulamento-de-comunicacao-de-incidente-de-seguranca>. Acesso em: 22 fev. 2026.

BRASIL. Agência Nacional de Proteção de Dados (ANPD). *ANPD, MPF e Senacon recomendam que X impeça geração e circulação de conteúdos sexualizados indevidos por meio do Grok*. 20 jan. 2026. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-mpf-e-senacon-recomendam-que-x-impeca-geracao-e-circulacao-de-conteudos-sexualizados-indevidos-por-meio-do-grok>. Acesso em: 22 fev. 2026.

DATA PRIVACY BRASIL. *Contribuição Data Privacy Brasil – Regulamento de Comunicação de Incidente de Segurança com Dados Pessoais*.

DE LIMA, Cíntia Rosa Pereira. *Autoridade nacional de proteção de dados e a efetividade da Lei Geral de Proteção de Dados (Lei n. 13.709/2018 e as alterações da Lei n. 13.853/2019), o Marco Civil da Internet (Lei n. 12.965/2014) e as sugestões de alteração do CDC (PL 3.514/2015)*. São Paulo: Almeida, 2020.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006.

GRABOSKY, Peter. Meta-regulation. In: DRAHOS, Peter. *Regulatory Theory: Foundations and applications*. 2017, ANU Press, Canberra.

JONES, Joe; FISCHER, Luke; SANIUK-HEINIG, Cheryl; KANTHASAMY, Saz. *Privacy Governance Report 2024*. Portsmouth, NH: IAPP, 2024.

KLITOU, Demetrius. *Privacy-Invasive Technologies and Privacy by Design: Safeguarding Privacy, Liberty and Security in the 21st Century*. Leiden University: T.M.C. Asser Press, 2014.

LESSIG, Lawrence. *Code and other laws of cyberspace*. Nova Iorque: Basic Books, 1999.

MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS (MGI). *Governo sanciona ECA Digital e anuncia transformação da ANPD em agência reguladora*. Notícias, 18 set. 2025. Disponível em: <https://www.gov.br/gestao/pt-br/assuntos/noticias/2025/se/governo-sanciona-eca-digital-e-anuncia-transformacao-da-anpd-em-agencia-reguladora>. Acesso em: 15 fev. 2026.

PARENTONI, Leonardo Netto. *Por que confiar na Autoridade Nacional de Proteção de Dados?* Revista da Faculdade de Direito da UFMG: Belo Horizonte, n. 79, pp. 163-192, jul. /dez.2021.

PINTO JR, Helder Q; PIRES, Melissa Cristina Pinto. *Assimetria de Informações e Problemas Regulatórios*. Agência Nacional de Petróleo, 2000.

SIMON, F. C. *Meta-regulation in practice: beyond normative views of morality and rationality*. London: Routledge, 2017.

SENADO aprova regulamentação da inteligência artificial: texto vai à Câmara. Distrito Federal, Agência Senado, 10 de dezembro

de 2024. Disponível em: <https://www12.senado.leg.br/noticias/materias/2024/12/10/senado-aprova-regulamentacao-da-inteligencia-artificial-texto-vai-a-camara>. Acesso em: 13 de março de 2025.

SUPREMO TRIBUNAL FEDERAL (STF). *STF define parâmetros para responsabilização de plataformas por conteúdos de terceiros*. Notícias STF, 26 jun. 2025. Disponível em: <https://noticias.stf.jus.br/postsnoticias/stf-define-parametros-para-responsabilizacao-de-plataformas-por-conteudos-de-terceiros/>. Acesso em: 4 fev. 2026.

TOMASEVICIUS FILHO, Eduardo. *Marco Civil da Internet: uma lei sem conteúdo normativo*. Estudos Avançados v. 30. Faculdade de Direito da Universidade de São Paulo, p. 269-285, 2016.

VERBRUGGEN, Paul; HAVINGA, Tetty. *The Rise of Transnational Private Meta-Regulators*. Tillburg Law Review v. 21, p. 119, 2016.

12. DEVER DE DILIGÊNCIA DE ADMINISTRADORES E INTELIGÊNCIA ARTIFICIAL: DESAFIOS DA DELEGAÇÃO DE PODER DECISÓRIO AOS ALGORITMOS DIANTE DO RISCO DE RESULTADOS DISCRIMINATÓRIOS

Giovanna de Amorim Freitas

Mestra em Direito e Inovação pela Universidade Federal de Juiz de Fora (UFJF). Especialista em Direito Digital pelo Instituto de Tecnologia e Sociedade do Rio de Janeiro – ITS Rio em parceria com o Centro de Estudos e Pesquisas no Ensino do Direito da Universidade do Estado do Rio de Janeiro (CEPED/UERJ). Integrante do Grupo de Pesquisa Empresa, Desenvolvimento e Responsabilidade (EDRESP).

INTRODUÇÃO

A tomada de decisões empresariais, historicamente associada a deliberações colegiadas em espaços formais e densamente informados, passa por uma transformação significativa diante da incorporação de sistemas de inteligência artificial. O que antes exigia interação presencial, tempo e mediação humana direta, hoje pode ser viabilizado por meio de operações automatizadas, muitas vezes acionadas por poucos comandos e sustentadas por estruturas algorítmicas complexas.

Nesse contexto, o objetivo do artigo é analisar como o dever de diligência dos administradores de sociedades empresárias, tradicionalmente estruturado como obrigação de meio, deve ser reinterpretado à luz das novas dinâmicas tecnológicas, identificando parâmetros de cuidado, informação e supervisão compatíveis com esse cenário. Para tanto, adota-se metodologia de natureza qualitativa, com base em revisão bibliográfica nacional e estrangeira e análise normativa.

O trabalho se desenvolve em cinco momentos: inicialmente, examinam-se os fundamentos societários do poder de decisão e as

tensões decorrentes da separação entre propriedade e controle; em seguida, aborda-se a intransferibilidade das funções administrativas em diálogo com as práticas de delegação decisória à inteligência artificial; na sequência, analisa-se o dever de diligência como eixo central da responsabilidade dos administradores; posteriormente, investiga-se o fenômeno da discriminação algorítmica e seus determinantes; por fim, examina-se a regulação baseada em risco como instrumento de densificação desse dever.

A hipótese que orienta o estudo é a de que a incorporação da inteligência artificial não altera a imputação das decisões aos administradores, mas intensifica e especifica o conteúdo do dever de diligência, exigindo estruturas mais robustas de governança, controle e supervisão tecnológica.

1. FUNDAMENTOS SOCIETÁRIOS SOBRE O PODER DE DECIDIR NAS COMPANHIAS

Em uma reconstrução histórica crítica da evolução das companhias, John Micklethwait e Adrian Wooldridge (2003), na obra “A Companhia: uma breve história de uma ideia revolucionária”, não se limitam a uma abordagem meramente econômica ou jurídica do fenômeno. Ao contrário, ampliam o campo de análise ao evidenciar as múltiplas dinâmicas sociais que emergem com a consolidação da forma societária moderna.

Quando avançam para as primeiras décadas do século XX, os autores destacam a chamada revolução gerencial e atribuem à progressiva separação entre propriedade e controle um papel central na reorganização das estruturas de poder no interior das companhias (Micklethwait; Wooldridge, 2003), um movimento que pode ser compreendido, em termos contemporâneos, como uma inflexão decisiva no desenvolvimento da governança corporativa.

Como expressão simbólica dessa transformação, mencionam os arranha-céus erguidos no período, como o Singer Building, o Metropolitan Life Tower e o Woolworth Building, cuja relevância

ultrapassa os avanços arquitetônicos, projetando-se também como manifestações do prestígio e da centralidade das grandes corporações naquele período (Micklethwait; Wooldridge, 2003).

A magnitude dessa reconfiguração foi tal que impactou não apenas a forma de gerir as companhias, mas também a própria organização dos espaços urbanos, que passaram a ser redesenhados para acomodar essa nova classe de executivos, seus fluxos de trabalho e seus padrões de vida:

Os habitantes dessas torres começaram a tediosa tarefa de coordenar o fluxo de matéria-prima vinda dos fornecedores para chegar aos clientes. Em breve sua capacidade organizativa, como o domínio da venda a domicílio pela Singer, tornou-se em si mesma uma vantagem competitiva decisiva. Gradualmente, esses “Homens da Companhia” começaram igualmente a tomar as grandes decisões estratégicas. Todas as fusões exigiam do grupo gerencial central a racionalização da nova firma. (Micklethwait; Wooldridge, 2003, p. 147)

Não obstante a condução ordinária dos negócios por gerentes profissionais tenha se consolidado, à época e até hoje, como a forma mais eficiente de organização da atividade empresarial e de persecução do interesse social (Kraakman et al., 2020; Oliveira, 2022), a dissociação entre propriedade e controle também passou a configurar uma das fontes estruturais de oportunismo inerentes à forma societária (Frazão, 2011).

A separação entre a titularidade do capital social e a condução efetiva da empresa³⁶⁷ — objeto de sistematização clássica a partir da obra de Adolf Berle e Gardiner Means (1932) — implica o enfraquecimento de um mecanismo tradicional de alinhamento de incentivos, na medida em que o patrimônio pessoal dos administradores deixa de operar como principal fator de disciplina econômica.

Como observa Ana Frazão (2011, p. 87), tal dissociação “faz com que o incentivo econômico natural para uma boa gestão

367 A relação de agência é o ajuste sob o qual uma ou mais pessoas (principal) contrata uma outra pessoa (agente) para executar em seu nome um serviço que implique delegação de algum poder de decisão ao agente (Jensen; Meckling, 1976).

— o próprio patrimônio investido — seja inferior”, o que “aumenta consideravelmente o risco de utilização dos poderes de gestão para benefício próprio e não para o cumprimento dos fins sociais” (Frazão, 2011, p. 87).

Essa ambivalência estrutural — ao mesmo tempo condição de eficiência e vetor de risco — constitui um dos fundamentos centrais do Direito Societário, que se organiza precisamente para estruturar mecanismos de contenção dessas assimetrias, não apenas na relação entre acionistas e administradores, mas também nos conflitos entre acionistas controladores e minoritários, bem como entre a companhia e terceiros (Kraakman et al., 2020).

No ordenamento brasileiro, esse arranjo institucional se materializa, de forma expressa, na Lei nº 6.404/1976 (Brasil, 1976), Lei das Sociedades por Ações (LSA), que disciplina o regime jurídico das sociedades por ações e estrutura a administração das companhias abertas a partir da divisão entre conselho de administração e diretoria (art. 138), de modo que cabe ao primeiro a fixação da orientação geral dos negócios e o exercício de funções estratégicas (art. 142), enquanto à diretoria incumbe a gestão cotidiana e a representação da companhia (art. 143).

Este modelo dual busca não apenas racionalizar a tomada de decisões, mas também introduzir mecanismos internos de monitoramento e controle, especialmente por meio da separação entre funções estratégicas e executivas (Lamy Filho; Pedreira, 2017; Kraakman et al., 2020).

A posição institucional da administração, enquanto instância legalmente responsável tanto pela definição de diretrizes quanto pela sua execução, a projeta como o núcleo de exercício do poder societário (Armour; Eidenmueller, 2019). Por essa razão, é nesse espaço que se manifestam, de forma mais intensa, os riscos associados à assimetria informacional, à discricionariedade decisória e, no contexto contemporâneo, à crescente mediação tecnológica dessas decisões (Armour; Eidenmueller, 2019).

No Brasil, soma-se à clássica preocupação com o equilíbrio entre proprietários e gestores um elemento adicional de significativa relevância: a presença estruturante do acionista controlador. Em mercados marcados por elevada concentração acionária, como é o caso brasileiro, a dinâmica de poder no interior das companhias não se esgota na separação entre propriedade e controle, sendo profundamente condicionada pela atuação daquele que detém o controle societário (Guerreiro, 1986; Munhoz, 2012; Comparato; Salomão Filho, 2014).

Embora o desenho institucional da administração — especialmente no que se refere ao conselho de administração — incorpore uma racionalidade orientada à autonomia funcional e à supervisão independente da gestão, essa presunção é, na prática, tensionada pela influência exercida pelo acionista controlador (Guerreiro, 1986).

A capacidade de determinar a composição dos órgãos sociais, de destituir administradores e de influenciar, direta ou indiretamente, decisões estratégicas compromete a autonomia institucional desses agentes, deslocando o centro efetivo do poder decisório para além das instâncias formalmente incumbidas de exercê-lo (Guerreiro, 1986; Comparato; Salomão Filho, 2014).

Nesse cenário, a tomada de decisão empresarial deve ser compreendida a partir de uma perspectiva ampliada, que abrange os processos relacionados às funções centrais da administração, o que inclui a definição de diretrizes estratégicas, o monitoramento da gestão e a condução das atividades operacionais (Mertens, 2023), sem olvidar, contudo, da influência estruturante exercida pelo acionista controlador sobre os interesses que orientam tais decisões.

A tradicional problemática das assimetrias informacionais e dos conflitos de interesse passa a conviver com um novo vetor de complexidade quando se traz à discussão o uso de sistemas de inteligência artificial nos processos empresariais de tomada de decisão (Pinheiro; Rocha; Del Llano, 2024). Compreender, portanto, como se estruturam e se legitimam as decisões no âmbito da administração

societária constitui passo necessário para analisar, em seguida, os limites e as implicações da delegação de funções decisórias a essa tecnologia.

2. DELEGAÇÃO DECISÓRIA E GRADAÇÕES DA MEDIAÇÃO ALGORÍTMICA

O poder decisório atribuído à administração das companhias possui caráter juridicamente intransferível (Frazão, 2020). Isso significa que, embora os administradores possam se valer de estruturas auxiliares e de informações produzidas por terceiros, a decisão final permanece sob sua titularidade e responsabilidade.

No ordenamento brasileiro, a Lei nº 6.404/1976 (Brasil, 1976) estabelece, em seu art. 139, a vedação à transferência das atribuições legalmente conferidas aos órgãos de administração, o que impede que tais competências sejam outorgadas a outros órgãos da companhia, ainda que previstos em estatuto³⁶⁸. Assim, uma vez investidos, os administradores são pessoal e diretamente responsáveis pelo exercício de suas funções, razão pela qual não podem invocar delegação ou subdelegação como excludente de responsabilidade (Lamy Filho; Pedreira, 2017).

Essa limitação, contudo, não afasta a possibilidade de delegação funcional de atividades instrumentais ou preparatórias. Admite-se a constituição de órgãos auxiliares e o apoio técnico à tomada de decisão desde que não haja deslocamento do núcleo decisório, que permanece vinculado aos administradores (Lamy Filho; Pedreira, 2017).

Em todos esses casos, entretanto, o dever de diligência dos administradores se projeta sobre o processo como um todo, exigindo não apenas a decisão final, mas também o controle sobre as etapas que a antecedem.

368 Modesto Carvalhosa (1998) observa que a tentativa de deslocar competências do conselho para outro órgão da estrutura societária compromete a função deliberativa estratégica que lhe é própria, abrindo espaço para conflitos de competência e ineficiência na gestão.

Nesse espectro, a crescente utilização de sistemas de inteligência artificial amplia significativamente a capacidade analítica e informacional dos administradores, especialmente em contextos de processamento de grandes volumes de dados, mas também introduz novos desafios quanto à opacidade, à auditabilidade e aos potenciais vieses dos sistemas utilizados. Sob essa perspectiva, a IA não inaugura propriamente a delegação, mas intensifica e complexifica formas já existentes de mediação técnica da decisão.

A literatura jurídica brasileira já vem se debruçando sobre essas questões, com destaque das implicações da delegação — parcial ou ampliada — a sistemas tecnológicos para a definição dos contornos da responsabilidade dos administradores e evidenciam a responsabilidade desses agentes na escolha, implementação e monitoramento confiável da tecnologia (Frazão, 2020; Teffé, Medon, 2020).

Sob a perspectiva da literatura estrangeira, a análise do uso de sistemas de inteligência artificial na tomada de decisão notadamente no contexto societário tem convergido para classificações estruturadas a partir de um critério central: o grau de autonomia decisória atribuído aos sistemas³⁶⁹. Esse recorte permite compreender a incorporação

369 Gouvêa (2022), parte do debate contemporâneo sobre a relação entre IA e governança corporativa, dividindo sua análise em dois cenários: (i) uso fragmentado, no qual a adoção parcial de diversas tecnologias de automação computacional (*blockchain*, *smart contracts* etc) são utilizadas de forma fragmentada para cumprir funções ainda isoladas na governança corporativa; e (ii) uso concentrado, para o qual basta o uso generalizado de ferramentas de IA de padrão autônomo mesmo que de forma não totalmente integrada e não depende da substituição do conselho ou da diretoria. Esta classificação, tem como base a categorização proposta por Iris H-Y Chiu e Ernest Lim (2022), que, a partir do objetivo de observar até que ponto estruturas e processos sob a égide das corporações se deslocariam em resposta ao advento da CorpTech, propõem uma estrutura analítica dividida em: estrutura incremental/facilitatória, estrutura radical/disruptiva e estrutura fundamental/estrutural. Já Hilb (2020) distingue os níveis de utilização de sistemas de IA em cinco cenários, a partir da interação entre a inteligência humana e a máquina, o que denomina de inteligência sinérgica: Inteligência assistida, Inteligência aumentada, Inteligência amplificada, Inteligência autônoma e Inteligência autopoietica. Mertens (2023) e Moeslein (2018), adotam como ponto de partida a tomada de decisões corporativas ao nível do conselho de administração e convergem quanto à seguinte categorização: IA assistida, IA aumentada, e IA autônoma. Reyes (2021), através de uma abordagem sistêmica para responder a perguntas sobre a natureza e o escopo da personalidade jurídica para sistemas artificiais, insere no debate uma taxonomia da realidade dos negócios

da IA não como fenômeno uniforme, mas como uma continuação de arranjos decisórios, nos quais varia a intensidade da mediação tecnológica.

A partir desse critério, identifica-se, de forma relativamente consolidada, três modelos principais de integração da IA aos processos decisórios empresariais: (i) sistemas utilizados como instrumento de apoio à decisão humana; (ii) sistemas empregados como mecanismos de aconselhamento, com maior capacidade de influenciar a deliberação; e (iii) sistemas que operam como substitutos funcionais da decisão humana, assumindo, em maior ou menor medida, a condução do processo decisório.

Essa tipologia evidencia que a delegação tecnológica não se apresenta de forma binária, mas graduada, o que impõe uma análise diferenciada quanto à extensão do controle humano, à rastreabilidade das decisões e, sobretudo, à imputação de responsabilidade no âmbito da administração societária.

No primeiro modelo, os sistemas de inteligência artificial atuam predominantemente como ferramentas auxiliares (Parentoni, 2022), voltadas à automatização de tarefas operacionais, administrativas ou informacionais, sem qualquer transferência relevante de direitos decisórios (Moeslein 2018; Hilb, 2020; Mertens, 2023).

A decisão final permanece integralmente sob responsabilidade de agentes humanos (Moeslein 2018; Hilb, 2020; Parentoni, 2022; Mertens, 2023) e o sistema de inteligência artificial é utilizado, por exemplo, para organizar, cruzar e sistematizar informações relevantes à formulação de políticas corporativas, à avaliação de desempenho de áreas ou unidades da companhia e ao monitoramento do cumprimento de critérios previamente estabelecidos para recrutamento, promoção, precificação ou seleção de parceiros comerciais.

autônomos, composta por três grupos e seis categorias de negócios autônomos: (i) Tradicional Plus: (a) Principalmente Automatizado Operacionalmente e (b) Automação Gerencial Leve; (ii) Entidades de Negócios Distribuídos: (a) Hierarquia Mediadora Autônoma e (b) Principalmente Autônomo; e (iii) Entidades Autônomas: (a) Totalmente Autônomo e (b) Entidades Algorítmicas.

Ainda que o sistema não formule juízos autônomos, o modo como os dados são estruturados e apresentados pode influenciar escolhas que, na prática, impactam de forma desigual determinados grupos, reproduzindo exclusões já presentes na organização ou no mercado.

Esse modelo não altera de forma substancial a estrutura de poder decisório da companhia (Moeslein 2018; Mertens, 2023), porquanto seus impactos concentram-se na eficiência informacional, na melhoria dos mecanismos de controle e no suporte às funções de codireção e supervisão, sem tensionar categorias jurídicas tradicionais como deveres fiduciários, imputação de responsabilidade ou exercício do poder de controle (Hilb, 2020).

O segundo modelo corresponde a um estágio intermediário, no qual os sistemas de IA passam a exercer influência direta e contínua sobre o processo decisório, ainda que a decisão formal permaneça atribuída a agentes humanos (Parentoni, 2022).

Nessa configuração, a IA não se limita a executar tarefas ou fornecer dados, mas formula recomendações, classifica alternativas e projeta cenários que condicionam, de modo relevante, as escolhas a serem tomadas pelos administradores (Hilb, 2020; Moeslein 2018; Mertens, 2023).

Trata-se de um nível disruptivo, no qual considera-se a equivalência na percepção de capacidade entre humanos e tecnologia em relação a tarefas que exigem habilidades compostas, como a avaliação de adequação de perfis, a identificação de riscos reputacionais ou a mensuração de impactos sociais de determinadas estratégias, aproximando-se de tarefas que envolvem discricionariedade e valorações qualitativas (Chiu e Lim, 2022, p. 22).

Nesse modelo, embora os direitos formais de decisão não sejam integralmente transferidos à máquina, ocorre um deslocamento significativo do poder cognitivo (Parentoni, 2022), na medida em que a capacidade analítica da IA passa a moldar o conteúdo das decisões estratégicas, de controle e, em alguns casos, de gestão de pessoas.

Trata-se, portanto, de um estágio que já tensiona a centralidade da decisão humana e levanta questões relevantes sobre dependência tecnológica, vieses algorítmicos, transparência e *accountability*, ainda que sem eliminar completamente a supervisão humana³⁷⁰.

O terceiro modelo corresponde às hipóteses em que os sistemas de IA substituem de forma total ou quase total as fases do processo humano de tomada de decisões (Parentoni, 2022.). Neste cenário, a autonomia decisória do sistema é elevada, e a intervenção humana, quando existente, tende a ser residual, *ex post* ou meramente simbólica (Moeslein 2018; Mertens, 2023).

Do ponto de vista jurídico, esse modelo é o que apresenta desafios estruturantes (Chiu e Lim, 2022) mais significativos, pois desafia frontalmente a dinâmica da arquitetura do direito societário, como a imputação de deveres fiduciários, a responsabilização por danos, a legitimidade da decisão e a própria noção de interesse social (Chiu e Lim, 2022).

É o caso, por exemplo, de pessoas jurídicas serem confiadas à inteligência artificial para gerenciar e operar o objeto social com liberdade para celebrar contratos com terceiros ou executar ações com base em instruções codificadas após o cumprimento de condições (Chiu e Lim, 2022). Assim como acontece nas hipóteses de um conselho híbrido entre diretores humanos e artificiais e de um conselho artificial, que consiste na composição exclusivamente de um sistema (conselho fundido) de inteligência artificial ou de vários diretores artificiais (conselho artificial) (Mertens, 2023).

A classificação dos níveis de incorporação da inteligência artificial à tomada de decisão empresarial, tal como desenvolvida na literatura, revela-se menos como um critério de segmentação rígida — entre usos permitidos ou proibidos, ou entre delegação parcial e total — e mais como um instrumento analítico capaz de evidenciar a complexidade e a diversidade dos arranjos decisórios contemporâneos.

370 É neste estágio que, dada a maior autonomia do sistema, questiona-se como a responsabilidade ou a obrigação por danos é atribuída, se a IA deve ser tratada como uma pessoa jurídica e se deve lhe ser atribuídos direitos (Chiu e Lim, 2022).

Ao demonstrar que a mediação tecnológica se dá em graus distintos, esses estudos afastam abordagens simplificadoras e indicam que diferentes configurações de uso da IA demandam respostas jurídicas igualmente diferenciadas.

Nesse contexto, o presente trabalho adota essa tipologia não como fim em si mesma, mas como base para investigar, na sequência, os impactos dessas variações sobre o dever de diligência dos administradores, especialmente diante da delegação de poder decisório a sistemas algorítmicos e dos riscos de produção de resultados discriminatórios.

3. CONTRAPARTIDA AOS PODERES CONFERIDOS À ADMINISTRAÇÃO: A DEVIDA DILIGÊNCIA NO USO DE SISTEMAS DE IA

Garantir efetividade ao princípio do equilíbrio entre poder e responsabilidade constitui um dos principais desafios da regulação jurídica dos mercados (Frazão, 2020), especialmente em contextos nos quais o exercício do poder decisório se torna progressivamente mediado por estruturas técnicas complexas, como os sistemas de inteligência artificial.

Se, por um lado, tais tecnologias ampliam a capacidade informacional dos administradores, por outro, introduzem novos riscos e opacidades que tensionam os parâmetros tradicionais de responsabilização.

No direito societário brasileiro, a atribuição do poder de condução das companhias à administração, aliada ao reconhecimento da influência do acionista controlador, é acompanhada da previsão de mecanismos jurídicos destinados a conter abusos e disciplinar o exercício desse poder. Nesse contexto, a Lei nº 6.404/1976 (Brasil, 1976) estabelece limites tanto ao exercício do poder de controle quanto à atuação dos administradores, estruturando um regime de responsabilidade que opera como contrapartida à centralidade decisória desses agentes.

No que se refere à administração, a contrapartida ao amplo poder de gestão é a responsabilidade civil dos administradores, de natureza subjetiva, aferida a partir de critérios predominantemente objetivos. Tais critérios se materializam nos chamados deveres fiduciários, entre os quais se destaca o dever de diligência (Lamy Filho; Pedreira, 2017), núcleo normativo a partir do qual se avalia a correção do processo decisório.

O dever de diligência consiste em elemento fundamental da responsabilidade dos administradores, pois envolve a aferição da reprovabilidade da conduta com base em um padrão abstrato de cuidado (Lamy Filho; Pedreira, 2017). Conforme dispõe o art. 153 da Lei nº 6.404/1976, o administrador deve empregar, no exercício de suas funções, o cuidado e a diligência que todo homem ativo e probo costuma empregar na administração de seus próprios negócios.:

Trata-se de um modelo aberto e flexível, que permite ao intérprete densificar o conteúdo do dever à luz das circunstâncias concretas (Lamy Filho; Pedreira, 2017). A referência ao “homem ativo e probo”, inspirada no paradigma do *bonus pater familias*, não pressupõe conhecimento técnico absoluto, mas exige do administrador a capacidade de reconhecer os limites de sua expertise e de buscar informações e assessoramento adequados para a tomada de decisão, atuando com prudência, atenção e zelo compatíveis com o padrão esperado de um gestor diligente (Lamy Filho; Pedreira, 2017).

Nesse sentido, como observa Frazão (2020), o dever de diligência não se confunde com a obtenção de resultados ótimos, mas se orienta fundamentalmente pela qualidade do processo decisório, razão pela qual é tradicionalmente compreendido como uma obrigação de meio, e não de resultado. Essa centralidade do processo — e não apenas da decisão final — revela-se especialmente relevante em contextos nos quais a formação da vontade decisória passa a depender, em maior ou menor medida, de sistemas algorítmicos, cuja lógica interna nem sempre é plenamente acessível ou verificável pelos administradores (Frazão, 2020).

Ao analisar o instituto, Pinheiro (2017) destaca sua fluidez e caráter casuístico, o que reforça a necessidade de uma interpretação contextualizada do dever de diligência, particularmente diante de novos arranjos decisórios mediados por tecnologia:

Na condição de cláusula geral, o dever de diligência é dotado de considerável fluidez, decorrente da dificuldade de previsão completa de todas as possíveis consequências e subdeveres dos gestores, diante da assunção de riscos que é inerente à própria atividade.(Pinheiro, 2017, p. 104)

Não obstante o reconhecimento do certo grau de abstração que a interpretação do dever de diligência exige, Pinheiro (2017) esclarece que a conduta dos administradores deve ser pautada pela boa-fé e acrescenta que, para além disso, deve resultar do sopesamento dos diversos interesses envolvidos na condução das atividades da sociedade empresária e do exercício de seus poderes de maneira informada com o conhecimento técnico e apropriado para a administração dos fins sociais.

Nesse sentido, o regime de responsabilidade civil dos administradores de sociedades empresárias, alicerçado no dever de diligência, funciona como instrumento jurídico essencial para limitar os riscos de abuso decorrentes de inovações organizacionais (Frazão, 2020). Em um cenário em que as estruturas empresariais se tornam progressivamente mais complexas, tecnológicas e fragmentadas, o dever de diligência passa a exigir dos administradores níveis proporcionais de cuidado, informação e supervisão, compatíveis com os riscos inerentes ao modelo decisório adotado.

A questão que então se coloca é se — e em que medida — o conteúdo do dever de diligência se transforma diante da incorporação de sistemas de inteligência artificial aos processos de tomada de decisão empresarial.

A incorporação de sistemas de inteligência artificial aos processos decisórios empresariais não altera, em sua base, o regime jurídico de responsabilidade dos administradores, mas tensiona de

forma significativa os critérios a partir dos quais o dever de diligência deve ser interpretado e aplicado.

Se, por um lado, permanece íntegra a premissa de que a decisão — ainda que mediada por sistemas tecnológicos — é imputável ao administrador, por outro, a crescente complexidade técnica e a opacidade desses sistemas deslocam o foco da análise para a qualidade do processo decisório que antecede a deliberação final.

Nesse contexto, a literatura converge no sentido de que a utilização de IA não exonera, mas antes intensifica as exigências associadas ao dever de diligência. Como destacado por Frazão (2020), mesmo em cenários de automação ampliada ou de decisões integralmente apoiadas em sistemas algorítmicos, a imputação jurídica permanece vinculada ao administrador, que, ao adotar ou cancelar os resultados produzidos, os incorpora à esfera de sua responsabilidade.

Não há, portanto, espaço para uma dissociação entre decisão e responsabilidade, sob pena de se instaurar um quadro de “irresponsabilidade organizada”, em que a complexidade técnica opera como fator de obscurecimento das reais alocações de poder (Frazão, 2020).

A partir dessa premissa, o dever de diligência passa a ser concretizado por meio de exigências específicas relacionadas ao uso de sistemas de IA, que se projetam sobre diferentes momentos do processo decisório (Teffé; Medon, 2020). Em primeiro lugar, destaca-se a necessidade de uma escolha informada e prudente da tecnologia a ser empregada, o que pressupõe a compreensão, ao menos em nível funcional, de suas capacidades, limitações e riscos (Frazão, 2020).

Nessa linha de raciocínio, a adoção de sistemas cuja lógica decisória se apresenta como uma “caixa-preta”, inacessível ou incompreensível para os próprios administradores, revela-se incompatível com o padrão de cuidado exigido, na medida em que inviabiliza a formação de uma decisão devidamente informada (Frazão, 2020).

Em segundo lugar, a diligência não se esgota na escolha do sistema, estendendo-se ao seu acompanhamento contínuo (Teffé;

Medon, 2020). A delegação de funções a sistemas algorítmicos não afasta o dever de supervisão, impondo aos administradores o monitoramento dos resultados produzidos, a verificação de sua consistência e a capacidade de intervenção diante de eventuais falhas, desvios ou resultados inadequados (Frazão, 2020).

Nesse sentido, a confiança depositada nos sistemas deve ser necessariamente limitada e calibrada, não se admitindo uma adesão automática ou acrítica às recomendações ou decisões produzidas.

A responsabilidade empresarial em contextos de uso de inteligência artificial, está, dessa maneira, fortemente associada a fatores como o grau de confiança no sistema, a qualidade dos dados que o alimentam e o nível de adesão às suas recomendações para a aferição da diligência dos administradores (Teffé; Medon, 2020).

A atuação diligente, nesse cenário, envolve não apenas a tomada de decisões informadas e refletidas, mas também a adequada delegação de tarefas, a busca por assessoramento técnico e a manutenção de uma postura ativa e crítica em relação aos instrumentos utilizados (Teffé; Medon, 2020; Frazão, 2020).

Adicionalmente, a incorporação de sistemas algorítmicos tende a reconfigurar os próprios custos de agência nas companhias. Como observam Armour e Eidenmüller (2019), a redução da participação humana direta em determinados processos decisórios não elimina os problemas de agência, mas os desloca e amplia em nível estratégico, exigindo novas formas de supervisão e governança.

Nesse cenário, a diligência dos administradores passa a envolver, de forma crescente, a capacidade de mapear, compreender e monitorar os riscos associados ao uso de dados e algoritmos, o que demanda um esforço adicional de organização e controle.

Por fim, a centralidade do dever de diligência reafirma a impossibilidade de substituição integral da figura do administrador por sistemas de inteligência artificial. Ainda que tais sistemas possam desempenhar funções sofisticadas de análise ou recomendação, a aferição do cumprimento de deveres fiduciários — como diligência, lealdade e atuação no interesse social — permanece intrinsecamente

vinculada a agentes humanos, aos quais se atribui responsabilidade pessoal pelos efeitos das decisões tomadas (Pinheiro; Rocha; Del Llano, 2024).

Se, por um lado, permanece íntegra a premissa de que a decisão — ainda que mediada por sistemas tecnológicos — é imputável ao administrador, por outro, desloca-se o foco da análise para a qualidade do processo decisório que antecede a deliberação final, exigindo dos administradores uma atuação mais informada, cautelosa e ativa diante de sistemas cuja complexidade e opacidade desafiam os parâmetros tradicionais de controle e responsabilização.

4. VIÉSES E RESULTADOS DISCRIMINATÓRIOS

A crescente incorporação de sistemas de inteligência artificial à tomada de decisão empresarial tem sido frequentemente justificada pela promessa de maior eficiência, objetividade e racionalidade, em contraste com as limitações cognitivas e os vieses inerentes à decisão humana (Frazão, 2020).

Inserida em um mercado tecnológico em expansão, essa narrativa sustenta a ideia de que decisões algorítmicas seriam, em princípio, mais neutras e confiáveis, aptas a orientar estratégias empresariais com base em critérios estatísticos e no processamento de grandes volumes de dados (Frazão, 2020).

Todavia, essa pretensa neutralidade revela-se, em grande medida, ilusória. Os sistemas de IA operam a partir de dados e modelos construídos por seres humanos, de modo que os vieses presentes nos conjuntos de dados ou nas escolhas de modelagem tendem a ser reproduzidos — e, por vezes, amplificados — nos resultados gerados (Teffé; Medon, 2020).

Nesse sentido, a utilização de algoritmos não elimina o problema da discricionariedade, mas o desloca para camadas menos visíveis do processo decisório, frequentemente marcadas por opacidade e dificuldade de escrutínio.

No âmbito empresarial, essa dinâmica assume especial relevância, na medida em que decisões potencialmente lesivas — desde a seleção de candidatos até a definição de estratégias comerciais ou concessão de crédito — passam a ser, total ou parcialmente, mediadas por sistemas automatizados (Teffé; Medon, 2020).

A possibilidade de produção de resultados discriminatórios, seja em relação a terceiros, seja no interior da própria organização, evidencia que a racionalização dos processos decisórios por meio da IA não é neutra do ponto de vista jurídico, podendo implicar a violação de direitos e a geração de danos (Teffé; Medon, 2020). Nesse contexto, o problema da discriminação algorítmica deve ser compreendido não como uma falha accidental, mas como um risco estrutural associado ao uso de sistemas de IA, especialmente quando alimentados por bases de dados historicamente enviesadas ou quando operam sem níveis adequados de transparência e controle (Teffé; Medon, 2020).

Assim, se as decisões empresariais permanecem imputáveis aos administradores, ainda que mediadas por sistemas tecnológicos, o risco de produção de resultados discriminatórios passa a integrar o conjunto de fatores que devem ser considerados na aferição do dever de diligência. A utilização de inteligência artificial, portanto, não apenas amplia a capacidade decisória, mas também redefine o conteúdo do cuidado exigido, exigindo dos administradores uma postura ativa na identificação, compreensão e mitigação desses riscos.

A literatura tem destacado que as tecnologias de IA não se desenvolvem em um vazio social, mas são concebidas e operam em contextos historicamente marcados por desigualdades. Como observa Costa e Kremer (2022), os riscos associados a essas tecnologias, especialmente no que se refere à discriminação, decorrem diretamente de fatores humanos, como as escolhas de design, a seleção dos dados e as finalidades econômicas que orientam sua utilização. A discriminação algorítmica, portanto, não constitui uma anomalia, mas uma possibilidade inerente ao próprio processo de desenvolvimento e aplicação desses sistemas (Costa; Kremer, 2022).

Do ponto de vista técnico, os sistemas de IA operam a partir de modelos baseados em heurísticas e inferências estatísticas, estruturados em ciclos contínuos de coleta, processamento e utilização de dados para a formulação de decisões (Faleiros Júnior, 2020). Conforme descreve Faleiros Júnior (2020), esse processo envolve, de forma simplificada, três etapas: a coleta de dados que alimentam o sistema, o seu processamento e, por fim, a geração de respostas ou decisões a partir de padrões identificados. Esse ciclo é constantemente retroalimentado, de modo que novas decisões passam a influenciar os dados futuros, reforçando padrões previamente estabelecidos (Faleiros Júnior, 2020).

Nesse contexto, falhas em qualquer uma dessas etapas — seja na qualidade dos dados coletados, nos critérios de processamento ou na própria adequação da solução algorítmica ao problema — podem resultar na reprodução ou amplificação de vieses (Faleiros Júnior, 2020). A utilização de bases históricas enviesadas, por exemplo, tende a gerar decisões que replicam desigualdades preexistentes, conferindo-lhes aparência de neutralidade técnica, além disso, casos como algoritmos de seleção de candidatos que privilegiam determinados perfis em detrimento de outros, com base em padrões históricos de contratação, ilustram como decisões aparentemente objetivas podem, na realidade, incorporar e perpetuar discriminações estruturais (Faleiros Júnior, 2020).

Dessa forma, a compreensão do funcionamento dos sistemas de inteligência artificial evidencia que o risco de discriminação não se limita ao resultado final da decisão, mas está enraizado no próprio processo que a produz. Essa constatação reforça a centralidade do dever de diligência como instrumento de controle, exigindo dos administradores não apenas a avaliação dos *outputs* gerados, mas também uma atenção qualificada às condições sob as quais esses resultados são produzidos.

Importa destacar, ainda, que, apesar dos avanços recentes, os sistemas de inteligência artificial estão longe de atingir qualquer forma de autonomia cognitiva equiparável à humana (Faleiros Júnior,

2020). Como observa Faleiros Júnior (2020), mesmo os modelos mais sofisticados, como aqueles baseados em *deep learning*, operam a partir de heurísticas computacionais e de processos decisórios fundados na análise de dados e em inferências estatísticas — o que a doutrina descreve como “predição por números”.

A chamada “singularidade tecnológica”, nesse sentido, permanece como uma hipótese distante, não sendo possível atribuir aos sistemas atuais qualquer forma de intencionalidade ou agência autônoma (Borges; Faleiros Júnior, 2023).

A produção de resultados discriminatórios não decorre de uma suposta “vontade” dos algoritmos, mas dos vieses incorporados ao longo de seu ciclo de desenvolvimento, alimentação e utilização (Borges; Faleiros Júnior, 2023). Não se trata, portanto, de algoritmos intrinsecamente discriminatórios, mas de sistemas que reproduzem — e, por vezes, amplificam — padrões previamente existentes, cuja origem remonta às decisões humanas que os estruturam e operam (Borges; Faleiros Júnior, 2023).

Nesse contexto, a responsabilidade pelos resultados produzidos permanece inequivocamente vinculada aos agentes envolvidos em sua concepção, implementação e uso, especialmente aos administradores que optam por incorporar tais sistemas aos processos decisórios empresariais. A utilização de inteligência artificial, assim, não desloca o eixo da responsabilidade, mas reforça a necessidade de uma atuação diligente, capaz de antecipar, identificar e mitigar os riscos associados à reprodução de vieses.

Ademais, a inserção desses sistemas na chamada economia de dados — marcada pela extração e exploração massiva de informações comportamentais — intensifica relações de poder e pode reforçar assimetrias sociais já existentes (Costa; Kremer, 2022).

A lógica subjacente a esses modelos amplia o potencial de impactos discriminatórios, especialmente quando decisões empresariais relevantes passam a ser orientadas por padrões estatísticos que refletem desigualdades estruturais.

Diante desse cenário, os vieses algorítmicos devem integrar, de forma central, o conteúdo do dever de diligência dos administradores, especialmente no que se refere à escolha, implementação, monitoramento e revisão contínua dos sistemas utilizados. A diligência, nesse contexto, não se limita à adoção de tecnologias eficientes, mas exige uma postura crítica e informada quanto aos riscos de discriminação que tais sistemas podem produzir, reafirmando o caráter processual e preventivo desse dever.

5. O RISCO COMO PARÂMETRO NORMATIVO

A crescente difusão de sistemas de inteligência artificial em múltiplos contextos decisórios tem sido acompanhada por um movimento regulatório orientado à antecipação e gestão de riscos. Diferentemente de abordagens tradicionais centradas exclusivamente na responsabilização posterior, iniciativas contemporâneas passam a estruturar modelos normativos baseados na identificação prévia de riscos e na imposição de obrigações proporcionais ao seu potencial lesivo.

Nesse contexto, o risco assume papel central como critério de organização e intensidade da regulação, funcionando como parâmetro para a definição de deveres, controles e exigências aplicáveis ao uso de sistemas de inteligência artificial. Não se trata, contudo, da instituição de um regime autônomo de responsabilidade, mas de uma racionalidade normativa voltada à calibração ex ante de condutas, com vistas à prevenção de danos.

A regulação baseada em risco não substitui os regimes jurídicos tradicionais de responsabilização, tampouco redefine seus fundamentos. Ao contrário, atua como elemento de densificação dos deveres já existentes e oferece parâmetros adicionais para a aferição da adequação da conduta dos agentes em contextos marcados por elevada complexidade técnica e potencial de impacto social.

No caso brasileiro, essa diretriz é expressamente incorporada pelo Projeto de Lei nº 2.338/2023 (Brasil, 2023), fortemente inspirado

na experiência europeia, para o qual o nível de autonomia do sistema, o grau de risco associado à sua utilização, a natureza dos agentes envolvidos e as particularidades do regime jurídico aplicável, passam a orientar a aferição da responsabilidade à luz das novas configurações tecnológicas³⁷¹.

Tal opção normativa parte do reconhecimento de que, embora persistam incertezas relevantes quanto ao funcionamento e aos impactos dessas tecnologias, já existe um acúmulo significativo de evidências empíricas acerca de riscos concretos associados ao seu uso (Frazão, 2024), como destaca a Professora Ana Frazão (2024), que integrou a Comissão de Juristas responsável por elaborar a minuta que serviu de base para o Projeto de Lei 2338/2023:

Entretanto, o Projeto de Lei nº 2338/2023 foi baseado na premissa de que, apesar do grau inquestionável de desconhecimento que ainda existe em relação à IA, já existe um mapeamento considerável na literatura e diversos estudos empíricos sobre vários de seus riscos. Um exemplo disso é a questão da discriminação algorítmica, que há muito deixou de ser um simples receio. De fato, existem inúmeras evidências de que situações como esta ocorreram repetidamente, com danos consequentes e graves para os pobres, mulheres, negros, crianças, adolescentes e outros grupos vulneráveis. (Frazão, 2024, p. 55 e 56, tradução nossa)

Não obstante, a literatura crítica tem apontado limitações relevantes desse modelo. Entre elas, destaca-se a tendência de associar a confiabilidade dos sistemas de inteligência artificial à mera aceitabilidade dos riscos que produzem, frequentemente aferida a partir de avaliações técnicas realizadas por especialistas (Laux; Wachter; Mottelstadt, 2024).

Esta aproximação pode obscurecer a distinção entre a confiabilidade dos sistemas — entendida como um processo contínuo de verificação e aprimoramento — e juízos normativos sobre o que se

371 Artigo 35, do PL 2338/2023.

considera aceitável em termos de risco (Laux; Wachter; Mottelstadt, 2024).

Além disso, a estrutura classificatória tende a operar com distinções relativamente rígidas entre níveis de risco, o que sugere uma separação estática entre aplicações aceitáveis e inaceitáveis (Laux; Wachter; Mottelstadt, 2024). Essa lógica binária mostra-se, contudo, pouco compatível com a natureza dinâmica e evolutiva dos sistemas de inteligência artificial, cujos riscos podem se modificar ao longo do tempo e conforme o contexto de sua utilização.

Ainda assim, para os fins deste trabalho, a categorização por risco oferece um ponto de partida relevante, porque além de estabelecer fronteiras definitivas entre o permitido e o proibido, ela fornece um repertório inicial de parâmetros capazes de orientar a identificação e a qualificação dos riscos envolvidos na tomada de decisão mediada por inteligência artificial.

Nesse sentido, a utilidade do modelo reside menos na sua pretensão classificatória e mais na sua capacidade de explicitar fatores que passam a integrar o conteúdo do dever de diligência.

Em outras palavras, ainda que insuficiente como critério exclusivo de regulação, a lógica da classificação por risco contribui para tornar mais visíveis os elementos que devem ser considerados pelos administradores na condução de processos decisórios mediados por sistemas de inteligência artificial, especialmente no que se refere à avaliação de impactos, à previsibilidade de danos e à necessidade de adoção de mecanismos de controle e supervisão.

5.1. Classificação de riscos e densificação normativa do dever de diligência

Se a regulação baseada em risco fornece um ponto de partida para a compreensão dos impactos da inteligência artificial, o seu verdadeiro potencial analítico reside na possibilidade de extrair, a partir dela, parâmetros concretos de cuidado aplicáveis à atuação dos agentes que se valem desses sistemas.

Nesse sentido, o Projeto de Lei nº 2.338/2023 (Brasil, 2023) não deve ser lido apenas como um instrumento de organização normativa, mas como um referencial a partir do qual se pode reconstruir o conteúdo exigível do dever de diligência em contextos de decisão mediada por inteligência artificial.

A propósito, a espinha dorsal da iniciativa regulatória repousa na proteção de direitos fundamentais das pessoas afetadas por esses sistemas (Frazão, 2024), com especial destaque para os princípios da igualdade, da não discriminação, da pluralidade e da diversidade. A partir dessa matriz, a classificação tripartite de riscos, que distingue entre riscos excessivos, altos e residuais, opera menos como um mecanismo de segmentação abstrata e mais como um indicativo do grau de cautela exigido na utilização da tecnologia em cada caso.

Uma das repercussões mais relevantes da classificação por risco projeta-se sobre a forma de estruturação dos regimes de responsabilidade civil (Frazão, 2024). Ainda que não haja uma ruptura com os modelos tradicionais, observa-se uma tendência de agravamento do regime aplicável conforme a intensidade do risco envolvido, admitindo-se, nas hipóteses mais sensíveis, a incidência de regimes mais rigorosos, como a responsabilização objetiva, e, nos demais casos, a manutenção da responsabilidade subjetiva acompanhada de mecanismos de facilitação probatória, a exemplo da presunção de culpa e da inversão do ônus da prova em favor da vítima (Frazão, 2024).

É precisamente a partir dessa qualificação que a lógica da classificação por risco revela sua utilidade prática: ao explicitar cenários em que os impactos potenciais são mais intensos, o modelo regulatório contribui para delimitar, com maior nitidez, os níveis de cautela exigidos dos agentes que se valem dessas tecnologias.

Nesse contexto, os chamados riscos excessivos são objeto de vedação expressa, a exemplo de sistemas destinados à exploração de vulnerabilidades de indivíduos ou grupos com potencial de causar

danos a direitos fundamentais³⁷². A opção por restringir essa categoria a hipóteses nas quais já há significativa convergência quanto à sua inadmissibilidade evidencia uma postura regulatória cautelosa, que reserva a proibição para situações em que o grau de risco ultrapassa os limites socialmente toleráveis (Frazão, 2024).

No que se refere aos sistemas classificados como de alto risco, o enquadramento decorre da probabilidade e da gravidade dos impactos adversos que podem gerar, especialmente em contextos decisórios sensíveis, como aqueles relacionados ao acesso ao trabalho ou a serviços essenciais³⁷³. Trata-se, portanto, de hipóteses em que a mediação algorítmica da decisão possui potencial significativo de afetar posições jurídicas relevantes, inclusive sob a perspectiva da produção de efeitos discriminatórios (Frazão, 2024).

Há uma delimitação negativa para esses casos, que exclui da categoria de alto risco os sistemas que não influenciam ou determinam resultados decisórios³⁷⁴. Nesse sentido, considerando-se que os administradores não podem abdicar de suas competências decisórias e que a decisão final lhes é juridicamente imputável, a utilização de sistemas de inteligência artificial tende, em alguma medida, a integrar o próprio processo de formação da vontade empresarial.

Ainda que formalmente apresentados como instrumentos auxiliares, tais sistemas influenciam a construção da decisão, especialmente quando operam a partir de análises complexas ou de difícil verificação pelos agentes humanos. Por conseguinte, a distinção entre sistemas que “influenciam” e aqueles que “determinam” resultados revela-se menos nítida quando observada à luz da dinâmica real dos processos decisórios empresariais.

A crescente dependência de *outputs* algorítmicos, sobretudo em contextos de elevada complexidade informacional, pode esvaziar, na prática, a ideia de intervenção humana como elemento suficiente para afastar o enquadramento em categorias de maior risco. O que

372 Artigo 13, do PL 2338/23.

373 Hipóteses do artigo 14, incisos III e IV, do PL 2338/23.

374 Artigo 14, parágrafo único, do PL 2338/23.

se observa, portanto, não é a substituição formal da decisão humana, mas a sua progressiva conformação por estruturas tecnológicas que condicionam, limitam ou orientam o espaço de escolha dos administradores.

Ainda assim, na hipótese de utilização de sistemas que se aproximam desses contextos de alto risco, o modelo regulatório estabelece um conjunto de exigências voltadas à estruturação de mecanismos internos de governança³⁷⁵.

Tais exigências abrangem, entre outros aspectos, a documentação das etapas relevantes do ciclo de vida do sistema, a realização de testes voltados à aferição de sua confiabilidade e segurança, a implementação de mecanismos de monitoramento contínuo de resultados — com especial atenção à identificação de padrões discriminatórios —, bem como a definição e o registro dos níveis de supervisão humana envolvidos na produção das decisões³⁷⁶.

Além disso, impõe-se a realização de avaliações de impacto algorítmico, que funcionam como instrumentos de antecipação e gestão de riscos, exigindo dos agentes envolvidos não apenas o conhecimento técnico sobre o sistema, mas também a capacidade de compreender seus potenciais efeitos sobre os indivíduos e grupos afetados.

Ainda nesse contexto, merece destaque a previsão de realização de avaliação preliminar de risco, facultada aos agentes de inteligência artificial antes da introdução ou utilização do sistema³⁷⁷. Embora a forma como está prevista hoje no Projeto de Lei não se trate de imposição, essa etapa assume relevância estratégica ao permitir não apenas a identificação do grau de risco envolvido, mas também a delimitação das obrigações que estão a ele vinculadas.

375 Artigo 18, do PL 2338/23.

376 O parágrafo traz uma síntese do conjunto de exigências voltadas à estruturação de mecanismos internos de governança especificamente pelo aplicador (aquele que emprega ou utiliza sistemas de inteligência artificial) ao introduzir ou colocar em circulação no mercado sistema de alto risco, conforme previsto no artigo 18, inciso I, do PL 2338/23.

377 Artigo 12, do PL 2338/23.

Sua realização projeta efeitos relevantes no plano da responsabilidade, na medida em que, se assim for aprovado, poderá servir como elemento de demonstração de conformidade, segurança e adoção de boas práticas.

Sob a perspectiva do dever de diligência, essa faculdade normativa adquire contornos ainda mais expressivos. A avaliação prévia de risco, embora formalmente opcional, tende a se converter em parâmetro relevante de aferição da conduta do administrador, especialmente em contextos nos quais os impactos potenciais da tecnologia são conhecidos ou previsíveis.

Em outras palavras, aquilo que o legislador apresenta como boa prática passa a integrar, no plano material, o conteúdo exigível do agir diligente, sobretudo quando sua ausência compromete a capacidade de compreensão e gestão dos riscos envolvidos e de comprovar a conformidade da organização.

O movimento analisado até aqui não se esgota na dimensão normativa. A doutrina há muito sinaliza a necessidade de construção de estruturas organizacionais capazes de internalizar o controle dos riscos associados ao uso de tecnologias complexas, especialmente por meio de mecanismos de governança e autorregulação (Faleiros Júnior, 2020; Teffé; Medon, 2020; Frazão, 2020).

Dentre elas, destaca-se a centralidade da revisão humana como instrumento de contenção de riscos, como forma de preservar a compatibilidade entre eficiência decisória e proteção de valores fundamentais (Parentoni, 2022).

Nesse sentido, a exigência de intervenção humana não se apresenta como regra absoluta, mas como mecanismo calibrado de controle, a ser acionado conforme a natureza e a intensidade dos riscos envolvidos (Parentoni, 2022). A possibilidade de monitoramento contínuo, revisão ou até mesmo anulação de decisões automatizadas desloca o controle humano para diferentes momentos do ciclo decisório, reforçando a ideia de que a supervisão não se limita ao instante final da decisão, mas se projeta sobre todo o funcionamento do sistema.

A sua adoção, contudo, não pode ser indiscriminada. A interferência humana implica custos e pode comprometer ganhos de eficiência, razão pela qual sua exigência deve ser reservada a contextos em que os riscos justificam tal medida, considerando fatores como a relevância dos direitos afetados, a reversibilidade das decisões e o grau de opacidade ou autonomia do sistema (Parentoni, 2022).

Em síntese, a incorporação de sistemas de inteligência artificial à tomada de decisão empresarial projeta, sobre o dever de diligência dos administradores, um conjunto mais denso e específico de exigências: compreensão mínima do funcionamento e das limitações dos sistemas utilizados; avaliação prévia dos riscos — inclusive discriminatórios — associados à sua aplicação; verificação da qualidade e governança dos dados empregados; adoção de mecanismos de documentação, rastreabilidade e testagem; implementação de estruturas de monitoramento contínuo e de mitigação de vieses; e definição de níveis adequados de supervisão humana, especialmente em contextos sensíveis.

Ainda que parte dessas medidas se apresente hoje sob a forma de boas práticas, sua progressiva positivação em iniciativas regulatórias — já obrigatórias em determinados contextos, como no mercado europeu — indica uma tendência de consolidação desses parâmetros como elementos integrantes do conteúdo exigível do dever de diligência.

CONSIDERAÇÕES FINAIS

A partir da reconstrução dos fundamentos societários do poder de decisão, evidenciou-se que a separação entre propriedade e controle, embora funcional à organização da companhia, sempre exigiu mecanismos de contenção de assimetrias e de responsabilização dos agentes incumbidos da gestão.

Demonstrou-se que o caráter intransferível das funções administrativas não impede a delegação de etapas do processo decisório, inclusive a sistemas de IA, mas preserva a imputação final

das decisões aos administradores. Ao incorporar a problemática da discriminação algorítmica, o estudo evidenciou que os riscos associados à IA não decorrem de uma suposta autonomia neutra da tecnologia, mas de fatores humanos incorporados aos dados, ao design e à aplicação dos sistemas.

Por fim, a análise da regulação baseada em risco permitiu identificar um movimento de densificação do dever de diligência. Ainda que tais iniciativas não instituem um novo regime de responsabilidade, elas tornam mais explícitos os parâmetros de cuidado exigíveis, como a avaliação prévia de riscos, a governança de dados, a rastreabilidade, o monitoramento contínuo e a supervisão humana. Nesse cenário, conclui-se que o dever de diligência se expande qualitativamente, pois passa a exigir dos administradores uma atuação informada, tecnicamente orientada e estruturalmente organizada para lidar com sistemas de alta complexidade e potencial de impacto.

Se, no início do século XX, a separação entre propriedade e controle encontrou expressão simbólica nos arranha-céus que materializavam o poder corporativo, hoje a centralidade da decisão desloca-se para infraestruturas tecnológicas menos visíveis, mas igualmente determinantes. As decisões já não dependem necessariamente de espaços físicos ou de deliberações presenciais, o que não esvazia — ao contrário, reforça — a necessidade de controle sobre como elas são formadas.

REFERÊNCIAS

ARMOUR, John; EIDENMUELLER, Horst. Self-Driving Corporations? **Harvard Business Law Review, European Corporate Governance Institute**, Law Working Paper, n° 475, 2019. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3442447. Acesso em: 18 jun. 2024.

BERLE, Adolf Augustus; MEANS, Gardiner. The Modern Corporation and Private Property. New York: Macmillan, 1932.

BORGES, Gustavo Silveira; FALEIROS JUNIOR, José Luiz de Moura. **Viés racial em sistemas de inteligência artificial: desafios para a responsabilidade civil e a necessidade de parametrização do risco**. Revista IBERC, v.6, n. 2, p. 100-128, maio/ago. 2023. Disponível em: <https://revista.iberc.org.br/iberc/article/view/237/217>. Acesso em: 7 abr. 2026.

BRASIL. **Lei nº 6.404, de 15 de dezembro de 1976**. Dispõe sobre as Sociedades por Ações. Brasília, DF: Diário Oficial da União, 1976b. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l6404compilada.htm. Acesso em: 22 ago. 2024.

BRASIL. Senado Federal. **Projeto de Lei nº 2.338, de 2023 (Substitutivo)**. Dispõe sobre o desenvolvimento, fomento, uso ético e responsável da Inteligência Artificial com base na centralidade da pessoa humana. Apresentado em 17 de março de 2025. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2868197&filename=PL%202338/2023. Acesso em: 23 mar. 2026.

CARVALHOSA, Modesto. **Comentários à Lei de sociedades anônimas**. São Paulo: Saraiva, 1998.

CHIU, Iris H-Y; LIM, Ernest WK. Technology vs ideology: how far will artificial intelligence and distributed ledger technology transform corporate governance and business? **Berkeley Business Law Journal**, v. 18, n. 1, 2020. Disponível: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3695006. Acesso em: 12 jul. 2024.

COMPARATO, Fábio Konder; SALOMÃO FILHO, Calixto. **O Poder de Controle na Sociedade Anônima**. 6. ed. Rio de Janeiro: Forense, 2014.

COSTA, Ramon; KREMER, Bianca. **Inteligência artificial e discriminação: desafios e perspectivas para a proteção de grupos vulneráveis frente às tecnologias de reconhecimento facial**. Revista Brasileira de Direitos Fundamentais & Justiça, 16 (1). Disponível em: <https://dfj.emnuvens.com.br/dfj/article/view/1316/1065>. Acesso em: 9 abr. 2026.

FALEIROS JÚNIOR. José Luiz de Moura. **Discriminação por algoritmos de inteligência artificial: a responsabilidade civil, os vieses e o exemplo das tecnologias baseadas em luminância**. Revista de Direito da Responsabilidade, 2020. Disponível em: <https://revistadireitoresponsabilidade.pt/2020/discriminacao-por-algoritmos-de-inteligencia-artificial-a-responsabilidade-civil-os-vieses-e-o-exemplo-das-tecnologias-baseadas-em-luminancia-jos-e-luiz-de-moura-faleiros-junior/>. Acesso em: 9 abr. 2026.

FRAZÃO, Ana. **Função social da empresa: repercussões sobre a responsabilidade civil de controladores e administradores de S/As**. Rio de Janeiro: Renovar, 2011.

FRAZÃO, Ana. **Regulation of artificial intelligence in Brazil: examination of Draft Bill nº. 2338/2023**. UNIO - EU Law Journal. v. 10, n. 1, mai. 2024, p. 54-69. Disponível em: https://www.researchgate.net/publication/382094171_Regulation_of_artificial_intelligence_in_Brazil_examination_of_Draft_Bill_no_23382023. Acesso em: 23 mar. 2026.

FRAZÃO, Ana. Responsabilidade civil de administradores de sociedades empresárias por decisões tomadas com base em sistemas de Inteligência Artificial. In: FRAZÃO, Ana; MULHOLLAND, Caitlin (org.). **Inteligência artificial e direito: ética, regulação e responsabilidade**. 2. ed. São Paulo: Thomson Reuters, 2020.

GUERREIRO, José Alexandre Tavares. Sociologia do poder na sociedade anônima. **Revista de Direito Mercantil: Industrial, Econômico e Financeiro**, n. 77, p. 50-56. Conferência pronunciada na Faculdade de Direito da Universidade Federal de Minas Gerais em 17 de março de 1986.

HILB, Michael. Toward artificial governance? The role of artificial intelligence in shaping the future of corporate governance. **Journal of Management and Governance**, Suíça, v. 24, n. 4, p. 851-870, 2020. Disponível em: <https://link.springer.com/article/10.1007/s10997-020-09519-9>. Acesso em: 8 de abril de 2024.

JENSEN, Michael C.; MECKLING, William H. Theory of the firm: Managerial behavior, agency costs and ownership structure. **Journal of Financial Economics**, v. 3, n. 4, p. 305-360, 1976. Disponível em: <https://www.sciencedirect.com/science/article/pii/0304405X7690026X>. Acesso em: 8 abr. 2025.

KRAAKMAN, Reinier et al. **A Anatomia do Direito Societário: uma abordagem comparada e funcional**. São Paulo: Editora Singular, 2020.

LAUX, Johann; WACHTER, Sandra; MOTTELSTADT, Brent. **Trustworthy artificial intelligence and the European Union AI act: On the conflation of trustworthiness and acceptability of risk**. Regulation & Governance, v. 18, n. 1., p. 3-32, January 2024. Disponível em: <https://onlinelibrary.wiley.com/doi/10.1111/regg.12512>. Acesso em: 4 jul. 2024.

MERTENS, Floris. The use of artificial intelligence in corporate decision-making at board level: a preliminary legal analysis. **Financial Law Institute**, 2023. Disponível em: <https://financiallawinstitute.ugent.be/wp-content/uploads/2023/11/2023-01.pdf>. Acesso em: 13 abr. 2024

MICKLETHWAIT, John; WOOLDRIDGE, Adrian. **A companhia: breve história de uma ideia revolucionária**. 1. ed. Rio de Janeiro: Objetiva, 2003.

MOESLEIN, Florian. Robots in the boardroom: artificial intelligence and corporate law. **Social Science Research Network Electronic Journal**, p. 649–670, 2017. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3037403. Acesso em: 18 mai. 2024.

MUNHOZ, Eduardo Secchi. Quem deve comandar a companhia? Alocação do poder empresarial: sistema de freios e contrapesos. **Temas essenciais de direito empresarial: estudos em homenagem a Modesto Carvalhosa**. São Paulo: Saraiva, 2012.

OLIVEIRA, Fabrício de Souza. **Governança corporativa - a crise financeira e os seus efeitos (equívocos e possibilidades)**. Rio de Janeiro: Processo, 2022.

PARENTONI, Leonardo. **What Should We Reasonably Expect From Artificial Intelligence?** SSRN Electronic Journal, p. 179-219. 2022. Disponível em: https://www.researchgate.net/publication/361988480_What_should_we_reasonably_expect_from_artificial_intelligence. Acesso em: 25 mar. 2024.

PINHEIRO, Caroline da Rosa. **Os impactos dos programas de integridade (compliance) sobre os deveres e responsabilidades dos acionistas controladores e administradores nas sociedades anônimas**. 2017. 318 f. Tese (Doutorado) – Programa de Pós-Graduação em Direito, Universidade do Estado do Rio de Janeiro, Rio de Janeiro,

2017. Disponível em: <https://www.bdttd.uerj.br:8443/handle/1/9346>. Acesso em: 25 mar. 2024.

PINHEIRO, Caroline da Rosa; ROCHA, Matheus Mazzoni; DEL LHANO, Larissa Almeida. Governança e Inteligência Artificial: (in) certezas sobre substituição humana nos conselhos de administração. In: XIII Encontro Internacional do CONPEDI Uruguai – Montevidéu, 2024. **Governo Digital, Direito E Novas Tecnologias** I. Disponível em: <https://site.conpedi.org.br/publicacoes/351f5k20/nhf03e63/LWCi1rkteY4fOjiA.pdf>. Acesso em: 20 fev. 2026.

TEFFÉ, Chiara Spadaccini de; MEDON, Filipe. Responsabilidade civil e regulação de novas tecnologias: questões acerca da utilização de inteligência artificial na tomada de decisões empresariais. **Revista Estudos Institucionais**, v. 6, n. 1, p. 301-333, 25 abr. 2020. Disponível em: <https://www.estudosinstitucionais.com/REI/article/view/383>. Acesso em: 17 abr. 2024.

13. O EQUILÍBRIO DELICADO: A PORTARIA MJSP Nº 961/2025 E A COMPATIBILIZAÇÃO ENTRE O USO DE TECNOLOGIA DA INFORMAÇÃO NA SEGURANÇA PÚBLICA E A PROTEÇÃO DOS DIREITOS FUNDAMENTAIS

Rafaela de Oliveira Lopes

Especialista em Direito Digital pelo Instituto de Tecnologia e Sociedade do Rio de Janeiro – ITS Rio em parceria com o Centro de Estudos e Pesquisas no Ensino do Direito da Universidade do Estado do Rio de Janeiro (CEPED/ UERJ).

INTRODUÇÃO

A segurança pública pode ser compreendida como a garantia dada pelo Estado de uma convivência social isenta de ameaça de violência, permitindo a todos o gozo dos seus direitos assegurados pela Constituição³⁷⁸. Nesta lógica, a Constituição Federal de 1988 estabelece a segurança pública como um dever do Estado, sendo simultaneamente um direito e responsabilidade de todos.

Por outro lado, o atual e inegável avanço da Tecnologia da Informação (TI) em todos os setores da sociedade reflete, inclusive, nos campos da segurança pública e da investigação criminal. Assim, para o combate às atividades criminosas, disseminou-se a adoção de ferramentas de inteligência artificial e soluções inovadoras como o reconhecimento facial³⁷⁹, ferramentas de controle por geolocalização (GPS), de processamento de dados informáticos (redes sociais, fotos,

378 DI PIERO, Mônica Maria Costa. Segurança Pública. Rev. Ministério Público, Rio de Janeiro, RJ, (19), 2004. Disponível em https://www.mprj.mp.br/documents/20184/2791465/Monica_Maria_Costa_Di_Piero.pdf Acesso em 10 de jul. 2025. Pág. 229.

379 PINHEIRO, Flávio Maria Leite. O papel da tecnologia e da inteligência artificial na segurança pública: desafios e convergências com os direitos fundamentais individuais e sociais. Revista do Ministério Público do Estado do Rio de Janeiro nº 94, out./dez. 2024. Disponível em https://www.mprj.mp.br/documents/20184/7377608/flavio_maria_leite_pinheiro.pdf Acesso em 15 jul. 2025. Pág. 58.

IP's, nuvens, e-mails e informações pessoais), de coleta por servidores de internet e de mensagens instantâneas, entre outros³⁸⁰.

É incontestado que a aplicação destas tecnologias aprimora a eficácia das investigações, otimiza a coleta e análise de informações e fortalece a segurança pública. Contudo, a aplicação indiscriminada acarreta, igualmente, vários questionamentos complexos relacionados, principalmente, à proteção dos direitos fundamentais dos cidadãos.

Revela-se, neste contexto, uma tensão entre a salvaguarda dos direitos fundamentais e o uso massivo de tecnologias de vigilância para aprimorar a segurança pública. Recentemente, foi editada a Portaria MJSP nº 961, de 24 de junho de 2025³⁸¹, através da qual o Ministério da Justiça e Segurança Pública estabeleceu diretrizes sobre uso de soluções de tecnologia da informação aplicadas às atividades de investigação criminal e inteligência de segurança pública.

O artigo propõe-se examinar o atual panorama do uso de TI na investigação criminal e inteligência de segurança pública com foco no estudo da citada Portaria, visando compreender aspectos como seu alcance normativo, fundamentos constitucionais e legais, fatores que levaram à sua edição, limites de uso e de acesso a dados, proteção de dados pessoais e privacidade, compatibilidade com outras normas e potenciais impactos que podem advir à proteção de direitos fundamentais.

Na elaboração do artigo foi empregado o método dedutivo, partindo de premissas gerais sobre o uso da tecnologia na seara da

380 VIEIRA, Andrey Bruno Cavalcante; SANTOS, Hugo Leonardo Rodrigues. Investigação criminal e tecnologias digitais: algumas reflexões sobre o policiamento preditivo e a admissibilidade de provas digitais. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, v. 11, n. 1, e1072, jan./abr. 2025. DOI: 10.22197/rbdpp.v11i1.1072. Disponível em: <https://revista.ibraspp.com.br/RBDPP/article/view/1072> Acesso em 15 jul. 2025. Pág. 9.

381 BRASIL. Ministério da Justiça e Segurança Pública. Portaria MJSP nº 961, de 24 de junho de 2025. Estabelece diretrizes sobre uso de soluções de tecnologia da informação aplicadas às atividades de investigação criminal e inteligência de segurança pública. Disponível em: https://www.in.gov.br/web/dou/-/portaria-mjsp-n-961-de-24-de-junho-de-2025-638661609?utm_campaign=tabuleiro_-_115&utm_medium=email&utm_source=RD+Station Acesso em 15 de jul. de 2025.

investigação criminal e inteligência de segurança pública para analisar o caso específico da Portaria.

1. A INFORMAÇÃO NA SOCIEDADE ATUAL

Transformações geopolíticas e econômicas significativas têm reconfigurado o papel da tecnologia no contexto social contemporâneo. A informação revela-se elemento estruturante da sociedade atual, cujas mudanças substantivas levaram diversos autores a defender uma nova configuração social: a sociedade da informação. Conforme Vieira e Santos (2025)³⁸²:

A “era da informação” denomina o período atual pós-industrial e/ou neoliberal, no qual a informação passou a exercer um papel central como novo padrão de acumulação de riquezas. Como opinou Thomas Stewart, o conhecimento agora é essencial em tudo o que produzimos e comercializamos, e gerenciar esse conhecimento se tornou crucial, uma vez que o capital intelectual, composto por conhecimento, informações, propriedade intelectual e experiência, é a matéria-prima para criar riqueza (1998, p. 11-23).

Esta sociedade repousa em novos marcos de desenvolvimento econômico, social e cultural decorrentes da globalização. As Tecnologias de Informação e Comunicação (TICs) permitem um novo paradigma no qual os indivíduos vivem em hiperconectividade permanente, disponíveis para se comunicarem a qualquer momento.

Segundo Bottino, Vargas e Prates (2023), a internet desponta como principal forma de comunicação com o mundo e fonte de

382 VIEIRA, Andrey Bruno Cavalcante; SANTOS, Hugo Leonardo Rodrigues. Investigação criminal e tecnologias digitais: algumas reflexões sobre o policiamento preditivo e a admissibilidade de provas digitais. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, v. 11, n. 1, e1072, jan./abr. 2025. DOI: 10.22197/rbdpp.v11i1.1072. Disponível em: <https://revista.ibraspp.com.br/RBDPP/article/view/1072> Acesso em: 20 jan. 2026.

aquisição de conhecimento e, concomitantemente, formam-se bancos de dados massivos e surge o conceito de *big data*³⁸³:

Era dada a largada para a formação de bancos de dados massivos pelas empresas de tecnologia, a grande matéria-prima do atual monopólio econômico das Big Techs — grandes empresas associadas a plataformas de uso intensivo de dados, que se constituem em uma das principais arenas de embates geopolíticos deste século, tendo como ponto nodal o fenômeno do *big data*. O ato de captar, armazenar e analisar dados não é algo novo na história da humanidade, mas vem se transformando ao longo da trajetória do desenvolvimento tecnológico. O grande crescimento do número de pessoas e dispositivos conectados à rede mundial de computadores, aliado ao exponencial barateamento dos custos para armazenamento de dados, tornam a quantidade de informação gerada e armazenada crescente a cada dia. (...)

Esse cenário está interligado ao *big data* e já se reflete na realidade empresarial e nos serviços públicos (...).

O presente estudo não possui a pretensão de esgotar o tema, ou oferecer uma definição final sobre o disputado conceito de *big data*. No entanto, após uma leitura detida sobre suas aplicações e funções nos mais diversos campos de conhecimento, dentro e fora do direito, entende-se por *big data* a análise de grandes quantidades de dados, realizada de maneira automatizada por algoritmos, com intuito de extrair resultados e benefícios (Gomes, 2019, p. 29). Isso vislumbrando-se ainda que *big data* é menos sobre dados e mais sobre a capacidade de pesquisa, agregação e referência cruzada de grandes conjuntos de dados (Boyd e Crawford, 2012).

As tecnologias baseadas em dados ditaram o desenvolvimento tecnológico dos últimos anos. A área de Inteligência Artificial

383 BOTTINO, T.; VARGAS, D.; PRATES, F. Segurança pública na era do *big data*: mapeamento e diagnóstico da implementação de novas tecnologias no combate à criminalidade. Rio de Janeiro: FGV Direito Rio, 2023. Disponível em <https://repositorio.fgv.br/server/api/core/bitstreams/869f434b-4ea1-4b73-ae69-983cde99e084/content>. Págs. 20 e 22. Acesso em 20 de jan. de 2026.

(IA)³⁸⁴, em especial o campo de *machine learning*, aproveita dados e algoritmos para permitir que os sistemas de IA aprendam e melhorem de maneira semelhante aos humanos, aprimorando progressivamente sua precisão ao longo do tempo. Esta tecnologia permite processar grandes quantidades de dados históricos, identificar padrões e prever novas relações entre dados até então desconhecidos³⁸⁵.

Este panorama viabiliza o desenvolvimento de ferramentas para o combate à criminalidade, exigindo das autoridades a aplicação de tecnologias de tratamento de dados à atividade policial e à persecução penal. O processo comporta duplo desafio: compatibilizar os riscos e benefícios inerentes ao emprego de tecnologias na segurança pública e superar os obstáculos para a regulação adequada do uso dessas ferramentas pela administração estatal. Isto porque, conforme ressaltam Vieira e Santos (2025):

Tecnologias avançadas como as utilizadas atualmente permitem que ferramentas digitais funcionem como meios de controle social altamente precisos, embora manipuláveis e de difícil compreensão, as quais escondem decisões políticas que controlam os parâmetros de conteúdo e funcionamento de programas eletrônicos.

1.1. Uso da tecnologia da informação na investigação criminal e na inteligência de segurança pública

São diversas as possibilidades de uso da tecnologia da informação como ferramenta no combate à criminalidade. O uso do *big data* associado a análises preditivas via IA ultrapassou a fantasia e

384 Segundo a Lei de Inteligência Artificial da União Europeia (Regulamento UE 2024/1689), um sistema de IA é um sistema baseado em máquinas concebido para funcionar com níveis de autonomia variáveis, e que pode apresentar capacidade de adaptação após a implantação e que, para objetivos explícitos ou implícitos, e com base nos dados de entrada que recebe, infere a forma de gerar resultados, tais como previsões, conteúdos, recomendações ou decisões que podem influenciar ambientes físicos ou virtuais". (UNIÃO EUROPEIA, 2024) Disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32024R1689> Acesso em 25 de jan. de 2026.

385 AMAZON WEB SERVICES. O que é machine learning? AWS, [s.d.]. Disponível em: <https://aws.amazon.com/pt/what-is/machine-learning/> Acesso em 25 de jan. de 2026.

já existem recursos tecnológicos aptos para antecipar a informação de ocorrência de delitos. Assim, o desenvolvimento de mecanismos de IA para a análise estratégica de dados permitiu que o *big data* fosse incorporado ao combate à criminalidade, aprimorando diretamente a atividade policial e a persecução penal. Conforme indicam Bottino, Vargas e Prates (2023)³⁸⁶:

O *big data* também tem sido utilizado no campo da prevenção e controle na segurança pública, situação em que é mobilizado para refletir de forma abrangente as características quantitativas do crime, peculiaridades do tempo e do espaço em que ele se insere, além de eventuais processos de mudança observáveis dentro de um período. Alguns autores têm denominado esse campo de atuação como *big data* criminal, cujo valor se reflete principalmente em práticas consideradas inovadoras para a prevenção de crimes (Cai, Li e Wang, 2020, p. 2).

Nos Estados Unidos, por exemplo, empregou-se o *big data* para analisar casos históricos de crimes e reconhecer tendências e padrões de repetição, utilizaram-se tecnologias preditivas para identificar possibilidades de reincidência de infratores ou revisão de liberdade condicional aplicadas pelos sistemas de justiça, criaram-se ferramentas de análises de dados da IBM para otimizar a atuação da polícia e desenvolveram-se sistemas e *softwares* para prever locais de alto risco para cometimento de crimes³⁸⁷. Na China, a análise criminal com *big data*, denominada “policiamento da informação”, vem se consolidando com o objetivo de desenvolver um sistema de análise de dados criminais e previsão de tendência (Bottino; Vargas; Prates, 2023).

386 BOTTINO, Thiago; VARGAS, Daniel; PRATES, Fernanda (coords.). Segurança pública na era do big data: mapeamento e diagnóstico da implementação de novas tecnologias no combate à criminalidade Rio de Janeiro: FGV Direito Rio, 2023. Disponível em: <https://repositorio.fgv.br/server/api/core/bitstreams/869f434b-4ea1-4b73-ae69-983cde99e084/content> Acesso em: 20 jan. 2026.

387 Bottino, Vargas e Prates (2023) citam como exemplos a polícia de Santa Cruz, no estado da Califórnia, o estado de Maryland, a polícia da Carolina do Sul e o departamento da polícia de Los Angeles (*Idem*).

Nestes campos, a análise preditiva via IA objetiva minerar dados colhidos anteriormente para traçar tendências futuras, o que impacta diretamente no desenvolvimento das políticas de segurança³⁸⁸. Segundo Vieira e Santos (2025):

É o que se dispõe a oferecer a análise preditiva via IA, com técnicas de *machine learning* (ML) – “área da inteligência artificial (IA) e da ciência da computação que se concentra no uso de dados e algoritmos para imitar a maneira como os humanos aprendem, melhorando gradualmente sua precisão” (IBM, 2023) – com a finalidade de minerar dados colhidos anteriormente (como relatórios policiais e registros de ocorrência) [...] Através do processamento dos dados, com métodos estatísticos aplicados a algoritmos treinados para fazer classificações ou previsões, traçam-se tendências futuras, influenciando diretamente nas práticas de policiamento, seja no desenvolvimento de estratégias de segurança pública seja por meio da escolha de alocação de recursos. Nesse contexto, surgiu o policiamento preditivo, que diz respeito a “sistemas computadorizados cujo processamento de informações por algoritmos se utilizam tanto de bancos de dados robustos quanto de análises estatísticas para fins de predição de um acontecimento criminoso futuro” (Moraes, 2022, p. 35 *apud* Vieira e Santos, 2025).

Todavia, esta tendência deve ser vista com cautela. É inequívoco o impacto das inovações tecnológicas sobre o direito criminal, em especial no que tange às investigações. Porém, o emprego de modelos estatísticos com o objetivo de prever comportamentos humanos pode perpetuar preconceitos e enviesamentos sociais. Ademais, a identificação de vestígios através da tecnologia afeta a lógica dos procedimentos e evidências, acarretando debates sobre os impactos

388 Segundo Bottino, Vargas e Prates (2023), “o policiamento preditivo associa técnicas computacionais sofisticadas, bancos de dados massivos (*big data*) e a estatística e oferece muitas promessas para a adoção de estratégias policiais mais efetivas à segurança pública. É o caso da predição de crimes, de ações para redução da criminalidade e até mesmo do perfil de sujeito que pode vir a cometer um delito. Trata-se de um desejo antigo de gestores públicos e forças policiais que começou a ganhar atenção no início dos anos 2010, quando algumas cidades nos Estados Unidos passaram a testar e utilizar esse tipo de ferramenta no trabalho policial.”. *Idem*, pág. 34-35.

no sistema legal e nos direitos individuais dos investigados (Vieira; Santos, 2025).

Assim, são recorrentes questionamentos³⁸⁹ sobre invasão de privacidade, coleta massiva de dados, geração de um ambiente de vigilância excessiva, riscos de erros (como falsas associações que podem prejudicar indivíduos inocentes) e a reprodução de desigualdades sociais e raciais que impactam negativamente determinados grupos³⁹⁰. Conforme pontuam Bottino, Vargas e Prates (2023):

O *big data* tem se mostrado uma janela de oportunidades para a solução de alguns dos principais desafios que se arrastam no campo da segurança pública, conferindo centralidade às realidades enfrentadas por cada força policial em termos de demanda, regionalidade e

389 Ressalta-se que o uso da tecnologia também pode trazer oportunidades de desenvolvimento para o ambiente penal. Segundo Campelo (2025), “Apesar dos desafios, a tecnologia também oferece oportunidades únicas para modernizar o sistema penal. Sistemas eletrônicos de monitoramento, como tornozeleiras, permitem alternativas à prisão preventiva, reduzindo a superlotação carcerária. Ferramentas de análise de dados também podem melhorar a gestão do sistema prisional, ajudando a identificar necessidades e otimizar recursos. Essas ferramentas também podem ser aplicadas na prevenção de crimes, utilizando dados estatísticos para planejar ações de segurança de maneira mais eficiente. A digitalização de processos judiciais é outro exemplo de modernização que beneficia o Direito Penal. Processos eletrônicos agilizam a tramitação, reduzem custos e aumentam a transparência, permitindo que partes interessadas acompanhem o andamento dos casos de maneira mais eficiente. Outras inovações incluem o uso de tecnologias de aprendizado de máquina para analisar jurisprudências e prever resultados de casos. Essas ferramentas podem ajudar advogados e promotores a construir argumentos mais robustos e a antecipar possíveis decisões judiciais. Além disso, tecnologias de análise forense avançada, como scanners 3D e reconstruções virtuais de cenas de crimes, estão permitindo investigações mais detalhadas e precisas”. In: CAMPELO, Marcelo. A influência da tecnologia no Direito Penal: desafios e oportunidades. Migalhas, seção Migalhas de Peso, 18 jan. 2025. Disponível em: <https://www.migalhas.com.br/depeso/422898/a-influencia-da-tecnologia-no-direito-penal-desafios-e-oportunidades>. Acesso em: 20 jan. 2026

390 Caldeira (2025) afirma que “A discriminação também é um risco comprovado, com estudos mostrando taxas de erro muito maiores em asiáticos e negros em comparação a brancos, além de desempenho inferior em mulheres e pessoas de pele escura, o que ameaça direitos fundamentais como igualdade, privacidade, liberdade de expressão e de reunião.” In: CALDEIRA, Rodrigo de Andrade Figaro. Inteligência artificial tem crescido na área de segurança pública. Consultor Jurídico, seção Opinião, 2 jul. 2025. Disponível em: <https://www.conjur.com.br/2025-jul-02/inteligencia-artificial-e-seguranca-publica-analise-critica-da-portaria-961-2025-do-mj-sp/>. Acesso em: 20 jan. 2026.

integração informacional. No entanto, não sem riscos. A inteligência artificial é uma tecnologia de propósito geral e de aplicações diversas, que carece de parâmetros de segurança determinados pelo Estado, na construção de uma relação de comando e controle. O cenário jurídico brasileiro atual, que já carece de uma legislação de proteção de dados pessoais aplicada ao contexto da segurança pública e persecução penal, ganha contornos ainda mais dramáticos no contexto da IA. Apesar dos inegáveis benefícios, tais aplicações trazem casos correntes de vieses de gênero, raça, classe, sexualidade e são capazes de potencializar os efeitos perigosos e perversivos da vigilância excessiva e do tecnoautoritarismo por parte dos agentes estatais.

(...)

A aplicação de sistemas de IA com aprendizado de máquina traz consigo grandes promessas para a solução de algumas das principais mazelas sociais, como o combate à violência, à letalidade e a garantia da segurança. No entanto, é essencial que o uso de quaisquer tecnologias na segurança pública e na esfera de persecução penal não sejam mais um fator de violação de direitos, razão pela qual a regulação se mostra tão importante para fins de segurança jurídica, garantia dos direitos fundamentais, gradação de riscos e responsabilização pelo uso da tecnologia de IA e seus impactos para a sociedade.

A frágil transparência no uso das soluções tecnológicas na seara criminal é destacada por Santos e Júnior (2025) nos seguintes termos³⁹¹:

A ausência de verificabilidade que caracterizam muitos sistemas algorítmicos comprometem o controle democrático sobre decisões automatizadas, contribuindo para o que Pasquale (2015) denominou “sociedade da caixa preta”. Nesse ambiente, escolhas decisórias escapam à supervisão institucional e ao escrutínio público, agravando o risco de expansão do Direito Penal por meio de uma lógica de antecipação e suspeição generalizada.

391 SANTOS, Bruno Cavalcante Leitão; JÚNIOR, Francisco de Assis de. A Portaria MJSP 961/2025 e os limites constitucionais ao uso da inteligência artificial na segurança pública. Boletim IBCCRIM, São Paulo, v. 33, n. 397, p. 18-21, dez. 2025. DOI: 10.5281/zenodo.17624181. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/2180/1538 Acesso em: 25 jan. 2026

É neste contexto que surge a Portaria MJSP nº 961, de 24 de junho de 2025³⁹², através da qual o Ministério da Justiça e Segurança Pública estabeleceu diretrizes sobre uso de soluções de tecnologia da informação aplicadas às atividades de investigação criminal e inteligência de segurança pública.

2. A PORTARIA MJSP Nº 961, DE 24 DE JUNHO DE 2025

2.1. Contexto e fundamentos legais da edição

O uso crescente e indiscriminado de tecnologias pelas forças de segurança gera preocupações e exige limites jurídicos e éticos. De acordo com Santos e Júnior (2025), a incorporação de sistemas automatizados nas atividades de investigação criminal e inteligência tem ocorrido “muitas vezes impulsionada por promessas de eficiência e predição, em um cenário de baixa regulamentação e escassa transparência”.

Atento a este cenário, em 30 de junho de 2025, o Ministério da Justiça e Segurança Pública publicou a Portaria nº 961/2025 com o objetivo de instituir normas regulamentares para a aplicação de tecnologias em atividades investigativas e de inteligência de segurança pública. A regulamentação inédita busca modernizar a atuação das instituições de segurança brasileiras, preservando simultaneamente os direitos fundamentais dos cidadãos³⁹³. A edição pelo Ministério da

392 BRASIL. Ministério da Justiça e Segurança Pública. Portaria MJSP nº 961, de 24 de junho de 2025. Estabelece diretrizes sobre uso de soluções de tecnologia da informação aplicadas às atividades de investigação criminal e inteligência de segurança pública. Disponível em: https://www.in.gov.br/web/dou/-/portaria-mjsp-n-961-de-24-de-junho-de-2025-638661609?utm_campaign=tabuleiro_-_115&utm_medium=email&utm_source=RD+Station Acesso em 15 de jul. de 2025.

393 Segundo Caldeira (2025), “[a Diretiva 680/2016 e o Regulamento 138/2024, ambos do Parlamento Europeu, serviram de inspiração tanto para a Portaria 961/2025, do MJSP, quanto para o anteprojeto da LGPD Penal e o Projeto de Lei 2.338/2023. Todavia, a normativa europeia foi muito mais exaustiva ao tratar o tema.”. In: CALDEIRA, Rodrigo de Andrade Figaro. Inteligência artificial tem crescido na área de segurança

Justiça e Segurança Pública fundamenta-se constitucionalmente no artigo 87, *in verbis*:

Art. 87. Os Ministros de Estado serão escolhidos dentre brasileiros maiores de vinte e um anos e no exercício dos direitos políticos.

Parágrafo único. Compete ao Ministro de Estado, além de outras atribuições estabelecidas nesta Constituição e na lei:

I - exercer a orientação, coordenação e supervisão dos órgãos e entidades da administração federal na área de sua competência e referendar os atos e decretos assinados pelo Presidente da República;

II - expedir instruções para a execução das leis, decretos e regulamentos;

O ato normativo fundamenta-se na competência para estabelecimento das Políticas de Segurança Pública e Defesa Social, cabendo à União Federal estabelecer a política nacional e aos Estados, ao Distrito Federal e aos Municípios a elaboração das suas respectivas políticas, conforme a Lei nº 13.675, de 11 de junho de 2018. Segundo o artigo 1º:

Art. 1º Esta Lei institui o Sistema Único de Segurança Pública (Susp) e cria a Política Nacional de Segurança Pública e Defesa Social (PNSPDS), com a finalidade de preservação da ordem pública e da incolumidade das pessoas e do patrimônio, por meio de atuação conjunta, coordenada, sistêmica e integrada dos órgãos de segurança pública e defesa social da União, dos Estados, do Distrito Federal e dos Municípios, em articulação com a sociedade.

A Portaria também menciona expressamente a Lei nº 14.600, de 19 de junho de 2023, que estabelece a organização básica dos órgãos da Presidência da República e dos Ministérios, notadamente o artigo 35:

Art. 35. Constituem áreas de competência do Ministério da Justiça e Segurança Pública:

pública. Consultor Jurídico, seção Opinião, 2 jul. 2025. Disponível em: <https://www.conjur.com.br/2025-jul-02/inteligencia-artificial-e-seguranca-publica-analise-critica-da-portaria-961-2025-do-mj-sp/>. Acesso em: 20 jan. 2026.]

XXI - desenvolvimento de estratégia comum baseada em modelos de gestão e de tecnologia que permitam a integração e a interoperabilidade dos sistemas de tecnologia da informação dos entes federativos, nas matérias afetas ao Ministério;

XXIII - tratamento de dados pessoais;

A regulamentação é uma antecipação do Poder Executivo ao Congresso Nacional, visto que ainda não há lei que disponha sobre o uso de novas tecnologias de informação em atividades de investigação criminal e inteligência de segurança pública. Neste contexto, é imperiosa a proteção dos dados pessoais dos indivíduos submetidos às investigações e há disposição expressa, na Lei Geral de Proteção de Dados Pessoais (LGPD - Lei nº 13.709 de 14 de agosto de 2018), quanto à sua inaplicabilidade para fins de segurança pública e atividades de investigação e repressão de infrações penais, exigindo a edição de legislação específica:

Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
(...)

III - realizado para fins exclusivos de:

- a) segurança pública;
 - b) defesa nacional;
 - c) segurança do Estado; ou
 - d) atividades de investigação e repressão de infrações penais; ou
- (...)

§ 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.

A LGPD Penal, normativo trará as regras sobre o tema³⁹⁴, ainda está em tramitação no Congresso Nacional no âmbito do Projeto de Lei

394 Garcia (2025) traz diversos elementos para explicar a ausência da LGPD Penal, como a garantia de espaços de atuação livre, a compreensão da lei como limitadora

nº 1515/2022³⁹⁵ e, atualmente, encontra-se para apreciação na Comissão de Ciência, Tecnologia e Inovação (CCTI). Em 30/10/2025 encerrou-se o prazo de 5 (cinco) sessões para apresentação de emendas ao projeto, não tendo sido apresentadas emendas³⁹⁶.

Outro normativo ainda não aprovado pelo Congresso e que pode trazer regras sobre o tema é o Projeto de Lei nº 2.338/2023, que trata da regulamentação da inteligência artificial³⁹⁷. O projeto foi remetido em 17/03/2025 à Câmara dos Deputados e, segundo a Casa Legislativa, é uma das prioridades para 2026³⁹⁸.

2.2. Alcance normativo e disposições principais

No capítulo das disposições preliminares são estabelecidos os órgãos aos quais a portaria se aplica (art. 1º), os valores que a norteiam

da atuação policial, heterogeneidade dos registros criminais entre estados, reduzida qualificação técnica de operadores em setores especializados e precária condição técnica e política para integração nacional de dados. GARCIA, Rafael de Deus. Ministério da Justiça avança na regulação da IA e se antecipa ao Congresso na LGPD penal. JOTA, seção Opinião & Análise, Artigos, 8 jul. 2025. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/mjssp-avanca-na-regulacao-da-ia-e-se-antecipa-ao-congresso-na-lgpd-penal> Acesso em 26 de jan. de 2026.

395 BRASIL. Câmara dos Deputados. Projeto de Lei n. 1.515, de 2022. Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais. Autor: Coronel Armando. Brasília, DF: Câmara dos Deputados, 2022. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2182274&filename=PL%201515/2022 Acesso em 20 de jan. de 2026.

396 BRASIL. Câmara dos Deputados. PL 1515/2022: ficha de tramitação. Brasília, DF: Câmara dos Deputados, 2022. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2326300#tramitacoes>. Acesso em: 20 de jan. de 2026.

397 BRASIL. Senado Federal. Projeto de Lei n. 2.338, de 2023. Dispõe sobre o uso da Inteligência Artificial. Autor: Senador Rodrigo Pacheco. Brasília, DF: Senado Federal, 2023. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/157233>. Acesso em: 20 jan. 2026.

398 CÂMARA DOS DEPUTADOS (@camaradosdeputados). O Marco Legal da Inteligência Artificial é uma das prioridades da Câmara dos Deputados em 2026. Instagram, reel, [s.d.]. Disponível em: <https://www.instagram.com/reel/DTwAnkXAaB8/>. Acesso em: 25 jan. 2026

(art. 2º), os objetivos (art. 3º) e conceitos (art. 4º). No capítulo da utilização das soluções de tecnologia da informação constam os limites e as finalidades autorizadoras (art. 6º), regras para obtenção de dados sigilosos (arts. 7º a 9º) e regras para uso de soluções de inteligência artificial (arts. 10 e 11). Há um capítulo das obrigações dos órgãos gestores (art. 12) e um dos registros da utilização das soluções (arts. 13 e 14). Por fim, o capítulo das disposições finais e transitórias (arts. 15 a 19) traz regras sobre responsabilização pelo uso indevido das soluções e a determinação de revisão e atualização dos atos normativos e instrumentos contratuais dos órgãos submetidos à portaria.

Assim sendo, quanto à aplicação, o normativo incide sobre todas as instituições de segurança pública federais, designadamente a Polícia Federal, a Polícia Rodoviária Federal, a Polícia Penal Federal, a Força Nacional de Segurança Pública e a Força Penal Nacional, bem como as secretarias nacionais de Segurança Pública (Senasp) e de Políticas Penais (Senappen). Igualmente, abrange os órgãos estaduais, distritais e municipais que recebem financiamento do Fundo Nacional de Segurança Pública e do Fundo Penitenciário Nacional, assim como o Conselho Administrativo de Defesa Econômica (Cade) e a Agência Nacional de Proteção de Dados (ANPD), no âmbito de suas respectivas atribuições³⁹⁹.

A portaria é considerada um marco para o setor por autorizar e estabelecer limites para o uso de tecnologias nas investigações criminais exigindo a observância de princípios relevantes como legalidade, necessidade e finalidade. Aliás, os princípios são mencionados como valores e como objetivos a serem alcançados.

O controle jurisdicional sobre as atividades é reforçado, por exemplo, ante a necessidade de decisão judicial específica para o acesso a dados sigilosos. Outro exemplo é o uso da tecnologia para localização e bloqueio de celulares usados para comunicações

399 BRASIL. Ministério da Justiça e Segurança Pública. Portaria do MJSP regulamenta uso de tecnologia em investigações criminais e inteligência de segurança pública. 30 jun. 2025. Disponível em: <https://www.gov.br/mj/pt-br/assuntos/noticias/portaria-do-mj-sp-regulamenta-uso-de-tecnologia-em-investigacoes-criminais-e-inteligencia-de-seguranca-publica> . Acesso em: 25 jan. 2026.

ilícitas dentro de presídios, cujo acesso aos dados armazenados nos dispositivos também demanda autorização judicial. Santos e Júnior (2025), argumentam ainda que:

ao exigir autorização judicial prévia ou hipóteses excepcionais, a Portaria garante um mecanismo de controle democrático sobre ferramentas que, em mãos desreguladas, poderiam corroer liberdades públicas e fomentar um Estado de vigilância .

Considerando a potencialidade da geração de riscos à privacidade e a outros direitos fundamentais, no que tange à governança e transparência no uso das soluções de tecnologia da informação, a regulamentação estabelece rigorosos requisitos. Desta forma, nos capítulos das obrigações dos órgãos gestores e de registro das utilizações há determinações expressas de controle de acesso aos sistemas, revisões periódicas dos perfis de usuários, planos de contingência e recuperação em caso de desastres, auditorias contínuas, investigação de acessos não autorizados e registro completo de todas as atividades realizadas, confira-se:

Art. 12. Os órgãos de segurança pública adotarão medidas técnicas, administrativas e organizacionais de segurança, em relação às soluções de tecnologia da informação sob sua gestão, a fim de garantir:

I - o controle de acesso, assegurando que apenas agentes no pleno exercício de suas funções e previamente autorizados possam ingressar nas respectivas instalações e utilizar as soluções, por meio da adoção de certificados digitais, biometria ou autenticação multifator;

II - a adoção e a revisão periódica de perfis, que definam papéis, privilégios e direitos de acesso às funcionalidades e às informações, assim como regras para a sua concessão e revogação;

III - a limitação do uso de perfis habilitados para atividades de inteligência a agentes com prerrogativas correspondentes e lotados em órgãos com tal atribuição;

IV - a elaboração de planos de contingência de segurança da informação e de recuperação de desastres, para que as soluções

de tecnologia da informação possam ser restauradas à condição imediatamente anterior ao incidente;

V - a transparência das contratações e a disponibilização de informações relevantes, atualizadas e íntegras sobre os processos licitatórios;

VI - o uso correto, ético e responsável das soluções de tecnologia da informação, promovendo capacitação aos usuários e adotando medidas para coibir o uso indevido das soluções sob sua responsabilidade pessoais;

VII - a continuidade das soluções de tecnologia da informação, promovendo sua evolução e manutenção adequada e avaliando periodicamente seus benefícios, necessidade, utilidade e uso;

VIII - a identificação e a investigação de casos de acessos indevidos, mediante a adoção de políticas de alerta contra usos maliciosos e atípicos das soluções de que trata esta Portaria; e

IX - a realização periódica de auditorias e do monitoramento de eficácia das medidas de segurança referidas neste artigo.

Parágrafo único. Os órgãos gestores assegurarão que a utilização das soluções de tecnologia da informação previstas nesta Portaria por outras entidades públicas será condicionada à adoção das medidas referidas neste artigo mediante assinatura de termos de responsabilidade.

Art. 13. Os órgãos de segurança pública devem registrar todos os acessos em log, contendo:

I - o nome e o CPF do usuário;

II - o endereço IP;

III - a data e a hora; e

IV - a natureza da operação, inclusive o histórico das consultas, sempre que tecnicamente viável.

Art. 14. Terão acesso aos registros de log as autoridades com competência legal para realizar o controle e assegurar o bom funcionamento das soluções de tecnologia da informação aplicadas às

atividades de investigação criminal e inteligência de segurança pública, assim como para verificar a legalidade de seu uso e a integridade e segurança dos dados.

A contratação de soluções tecnológicas pelos órgãos também é mencionada, reiterando-se a obrigatoriedade da transparência e a disponibilização de informações relevantes, atualizadas e íntegras, de forma a maximizar o controle social sobre os investimentos em tecnologia de segurança pública.

A portaria exige que o uso das soluções seja proporcional, observe o dever de prevenção de riscos e as leis aplicáveis à espécie e não resulte em lesão à vida e à integridade física das pessoas. Ademais, é vedado o uso que permita a identificação biométrica à distância, em tempo real, em espaços acessíveis ao público, salvo nos casos restritos definidos na própria portaria, quais sejam⁴⁰⁰:

Art. 11. Os órgãos de segurança pública poderão utilizar soluções de inteligência artificial, desde que de seu funcionamento e de suas capacidades não possa resultar lesão à vida e à integridade física das pessoas.

§ 1º É vedado aos órgãos referidos no caput utilizar soluções de inteligência artificial que permitam a identificação biométrica à distância, em tempo real, em espaços acessíveis ao público, exceto nos seguintes casos:

a) instrução de inquérito ou processo criminal, mediante autorização judicial prévia e motivada, quando houver indícios razoáveis da autoria ou participação em infração penal, a prova não puder ser feita por outros meios disponíveis e o fato investigado não constituir infração penal de menor potencial ofensivo;

400 BRASIL. Ministério da Justiça e Segurança Pública. Portaria MJSP nº 961, de 24 de junho de 2025. Estabelece diretrizes sobre uso de soluções de tecnologia da informação aplicadas às atividades de investigação criminal e inteligência de segurança pública. Disponível em https://www.in.gov.br/web/dou/-/portaria-mjsp-n-961-de-24-de-junho-de-2025-638661609?utm_campaign=tabuleiro_-_115&utm_medium=email&utm_source=RD+Station Acesso em 15 de jul. de 2025.

b) busca de vítimas de crimes, de pessoas desaparecidas ou em circunstâncias que envolvam ameaça grave e iminente à vida ou à integridade física de pessoas naturais;

c) flagrante delito de crimes punidos com pena privativa de liberdade máxima superior a dois anos, com imediata comunicação à autoridade judicial;

d) recaptura de réus ou detentos evadidos; ou

e) cumprimento de mandados de prisão ordenados pelo Poder Judiciário e das medidas e penas previstas no inciso II do art. 319 do Código de Processo Penal e no inciso IV do art. 47 do Código Penal.

§ 2º A utilização de soluções de inteligência artificial que não se enquadre nas hipóteses listadas no § 1º deste artigo deverá ser formalmente justificada e precedida de estudos que considerem os impactos negativos da inferência algorítmica.

Assim, de acordo com Santos e Júnior (2025), a previsão excepcional de permissões para o uso da identificação biométrica é sustentada por uma justificativa própria, formulada pelos autores nos seguintes termos

As permissões excepcionais previstas — busca de vítimas ou desaparecidos, flagrante de crimes graves, recaptura de presos e cumprimento de mandados judiciais — justificam-se por razões de elevado interesse público. Nesses casos, a intervenção tecnológica não se destina à vigilância generalizada, mas à proteção imediata da vida, da integridade física ou ao cumprimento de decisões judiciais. Justamente por isso, devem ser interpretadas de forma restritiva e aplicadas com rigor, de modo a evitar a banalização das exceções. A coleta de dados biométricos é especialmente sensível, pois permite rastreamento contínuo de indivíduos e pode viabilizar formas de controle incompatíveis com democracia (Zuboff, 2020).

Pelo exposto, a portaria se apresenta como a primeira normativa específica brasileira que estabelece parâmetros claros para o uso de soluções de tecnologia da informação no campo da segurança pública,

definindo limites éticos e operacionais para garantir eficiência e resguardar os direitos fundamentais dos cidadãos.

2.3. Impactos, lacunas e desafios da Portaria

Diante da crescente preocupação com o uso indiscriminado de sistemas digitais pelas forças de segurança, a Portaria MJSP nº 961/2025 representa um importante marco normativo inicial para proteger garantias constitucionais diante do avanço tecnológico que caracteriza o setor. Contudo, ela não é imune a críticas.

O primeiro aspecto a ser ressaltado é que nem todos os entes federativos submetem-se a ela, revelando a carência de força vinculante direta em certos casos. No artigo 2º verifica-se que os entes federativos que desenvolvam ou adquiram tecnologias com seus próprios recursos (ou seja, sem utilizar recursos oriundos do Fundo Nacional de Segurança Pública e do Fundo Penitenciário Nacional), por disposição expressa, não precisam se adequar à portaria.

Santos e Júnior (2025) oferecem um contraponto relevante a essa previsão normativa ao chamarem atenção para o fato de que a Portaria MJSP nº 961/2025 não deve ser compreendida apenas a partir de sua incidência imediata e formal. Neste diapasão, os autores argumentam que, embora a aplicação imediata da Portaria MJSP nº 961/2025 esteja circunscrita aos órgãos de segurança pública que recebem recursos federais, seus preceitos transcendem a dimensão orçamentária. Sustentam ainda que, sendo assim se revelam como parâmetro interpretativo para a aferição da constitucionalidade de políticas de vigilância nos níveis estadual e municipal (*idem*):

A União detém competência privativa para legislar sobre normas gerais de segurança pública (Brasil, 1988, art. 22, XXI e XXII), cabendo aos estados suplementarem-nas (art. 24, I e IX), em um modelo de responsabilidade compartilhada (art. 144).

A vinculação prevista no art. 1º, §2º, condiciona a observância da Portaria ao uso de recursos federais (Brasil, 2025b), conferindo-lhe eficácia normativa indireta. Ainda que não obrigue automaticamente

os estados, suas diretrizes funcionam como parâmetro constitucional interpretativo, sobretudo por envolverem direitos fundamentais.

(...)

A Portaria funciona, nesse cenário, como instrumento normativo de contenção e antecipação de riscos. Ainda que não substitua uma lei geral sobre IA, pode orientar a elaboração de normas federativas harmônicas com os princípios da dignidade humana, finalidade legítima e proteção de dados.

De todo modo, para fins de proteção das garantias constitucionais, o ideal seria a edição de lei que abrangesse inequivocamente todos os entes federativos. Outro ponto é que a simples edição da norma infralegal não garante sua efetividade, exigindo-se o fortalecimento de instituições capazes de monitorar seu atendimento e a aprovação de leis específicas. Conforme destacado pela Data Privacy Brasil⁴⁰¹:

A Portaria nº 961/2025 é um primeiro passo importante para a criação de um marco regulatório sobre tecnologias de vigilância, investigação e inteligência no Brasil. Ao vincular o uso de soluções de TI ao respeito a direitos fundamentais e exigir parâmetros mínimos para seu funcionamento, o Ministério da Justiça dá um sinal positivo de que está atento à complexidade e à relevância do tema [...]. [...] No entanto, a efetividade dessa norma dependerá da capacidade de implementá-la com transparência e fiscalização. O controle do uso de tecnologias como o Córtex e outras ferramentas intrusivas continuará desafiador sem o fortalecimento institucional de órgãos como o próprio MJSP e a Autoridade Nacional de Proteção de Dados (ANPD). A aprovação de legislações específicas, como a LGPD Penal, e o avanço no julgamento da ADPF 1143 pelo Supremo Tribunal Federal também serão cruciais para consolidar um ambiente jurídico que proteja a população e limite abusos estatais no uso de tecnologias.

401 DATA PRIVACY BRASIL. Tabuleiro #115 | Um primeiro passo na regulação do uso de tecnologias na segurança pública. Data Privacy Brasil, 18 jul. 2025. Disponível em: <https://dataprivacy.com.br/tabuleiro-115-um-primeiro-passo-na-regulacao-do-uso-de-tecnologias-na-seguranca-publica/> Acesso em 20 de jan. de 2026.

Em prosseguimento, também existem críticas à Portaria relacionadas a elementos passíveis de exame de constitucionalidade formal por possivelmente avançar sobre a competência da União em legislar sobre matéria processual penal⁴⁰² (Garcia, 2025).

A seu turno, Breier (2025) analisa a Portaria sob o prisma do risco à defesa técnica e à paridade de armas no processo penal. O autor entende que, apesar das diretrizes determinarem o respeito aos direitos fundamentais, diversos dispositivos impõem restrições significativas ao exercício pleno da advocacia e prejudicam o devido processo legal (Breier, 2025)⁴⁰³.

Desta forma, o normativo violaria diretamente o direito ao contraditório e ampla defesa insculpido no art. 5º, inciso LV, da Constituição Federal (Brasil, 1988)⁴⁰⁴ ao conferir às autoridades policiais privilégios como o acesso preferencial e unilateral a bancos de dados, sistemas de vigilância, ferramentas de reconhecimento facial e plataformas algorítmicas, não dispondo a defesa técnica das mesmas condições. Neste sentido, determina:

As violações se agravam em razão da omissão da Portaria quanto aos seguintes aspectos:

- Não assegura à defesa acesso técnico aos algoritmos e às inferências automatizadas utilizadas na identificação e produção de provas (art. 10);

402 “Art. 22. Compete privativamente à União legislar sobre: I - direito civil, comercial, penal, processual, eleitoral, agrário, marítimo, aeronáutico, espacial e do trabalho;”. BRASIL. 1988. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 25 jan. 2026.

403 BREIER, Ricardo. O Risco à Defesa Técnica e à Paridade de Armas no Processo Penal: Análise Crítica da Portaria MJSP nº 961/2025. Abracrim, seção Artigos, 15 jul. 2025. Disponível em: <https://web.abracrim.adv.br/o-risco-a-defesa-tecnica-e-a-paridade-de-armas-no-processo-penal-analise-critica-da-portaria-mjsp-no-961-2025/>. Acesso em: 25 jan. 2026.

404 “[Art. 5º Todos são iguais perante a lei [...] LV - aos litigantes, em processo judicial ou administrativo, e aos acusados em geral são assegurados o contraditório e ampla defesa, com os meios e recursos a ela inerentes” (BRASIL, 1988). BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 25 jan. 2026.]

- Não garante ciência prévia ou simultânea dos procedimentos de extração e análise de dados digitais, em afronta à cadeia de custódia prevista nos arts. 158-A a 158-F do CPP;

- Impede a fiscalização externa dos sistemas utilizados, concentrando o controle nos próprios órgãos de segurança (art. 12);

- Exclui a participação da defesa na construção dos parâmetros algorítmicos, contrariando o princípio da transparência epistêmica e da ciência aberta. (Brasil, 1988).

Quanto ao exercício da advocacia, o autor sustenta que restaria comprometido na medida em que o advogado não disporia de meios reais para a atuação defensiva, cabendo-lhe a mera possibilidade de contestação posterior de provas digitais produzidas de forma unilateral e sem ter, efetivamente, o acesso a dados, algoritmos e ferramentas de análise digital. Isto configuraria verdadeira assimetria técnico-probatória entre acusação e defesa.

Por fim, Breier (2025) também questiona a legitimidade da Portaria MJSP nº 961/2025 devido à elaboração sem participação democrática:

Outro ponto crítico reside na ausência de participação democrática na elaboração da norma. A Portaria foi editada sem consulta pública ou diálogo institucional com entidades como a OAB, Defensoria Pública e Abracrim. A imposição verticalizada de um novo modelo de justiça penal digital, sem o devido debate, compromete sua legitimidade democrática e constitucional.

CONSIDERAÇÕES FINAIS

O avanço da tecnologia da informação reconfigurou drasticamente a sociedade contemporânea e suas implicações para a segurança pública são profundas e complexas. A utilização de ferramentas como inteligência artificial e o *big data* e a criação de sistemas de policiamento preditivo possuem um potencial significativo para aprimorar a eficácia das atividades de investigação criminal e inteligência. Contudo, essa crescente digitalização das

práticas de segurança acarreta uma tensão com a salvaguarda dos direitos e garantias fundamentais, como a privacidade, a presunção de inocência e o devido processo legal.

Neste cenário, a edição da Portaria MJSP nº 961/2025 surge como uma iniciativa pioneira e relevante do Poder Executivo brasileiro para estabelecer um marco regulatório inicial. O normativo demonstra a preocupação em conciliar a imparável inovação tecnológica com os preceitos legais ao estipular princípios norteadores como a legalidade, a necessidade e a finalidade, além de impor requisitos de transparência, governança e controle sobre o uso dessas tecnologias. A exigência de autorização judicial para acesso a dados sigilosos e a restrição ao uso de identificação biométrica em tempo real são exemplos notáveis dessa busca por um equilíbrio.

Todavia, a análise aprofundada revela que a Portaria, apesar de seus méritos, constitui uma solução parcial e insuficiente para a magnitude dos desafios. Sua eficácia é limitada pela sua aplicabilidade restrita aos órgãos de segurança que recebem recursos federais, deixando uma lacuna regulatória significativa para as instituições que operam com financiamento próprio. E mais, sua efetividade demanda o fortalecimento de instituições capazes de monitorar seu atendimento.

Ademais, a norma é alvo de críticas quanto à sua elaboração, que careceu de um amplo debate público e da participação de atores essenciais da sociedade civil e do sistema de justiça, como a Ordem dos Advogados do Brasil e a Defensoria Pública. A potencial invasão de competência legislativa da União Federal, outro ponto de atenção, também é aventado por estudiosos.

As preocupações estendem-se ao campo processual, onde a portaria é questionada por potencialmente gerar uma assimetria de armas entre acusação e defesa ao conceder às autoridades policiais acesso privilegiado a ferramentas de análise de dados sem garantir à defesa as mesmas condições técnicas para o contraditório. Tal desequilíbrio ameaça a paridade processual e pode comprometer a integridade do sistema de justiça criminal.

Conclui-se, portanto, que a Portaria MJSP nº 961/2025 representa um passo inicial importante, mas que não esgota a necessidade de uma regulamentação robusta e abrangente. A complexidade do tema exige uma resposta do Poder Legislativo, por meio da aprovação de leis específicas como o projeto da LGPD Penal e o Marco Legal da Inteligência Artificial, ambos ainda em tramitação. Somente um arcabouço jurídico sólido, que vincule todos os entes federativos e estabeleça regras claras de governança, responsabilização e controle social, poderá assegurar que a tecnologia sirva como um instrumento para a promoção da justiça e da segurança, sem que isso ocorra em detrimento dos direitos fundamentais que constituem o alicerce do Estado Democrático de Direito.

REFERÊNCIAS

ARRUDA, Ana Julia Pozzi; RESENDE, Ana Paula Bougleux Andrade; FERNANDES, Fernando Andrade. Sistemas de policiamento preditivo e afetação de direitos humanos à luz da criminologia crítica. *Direito Público*, [S. l.], v. 18, n. 100, 2022. DOI: 10.11117/rdp.v18i100.5978. Disponível em: <<https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/5978>>. Acesso em: 15 jul. 2025.

AMAZON WEB SERVICES. O que é machine learning? AWS, [s.d.]. Disponível em: <<https://aws.amazon.com/pt/what-is/machine-learning/>>. Acesso em: 25 jan. 2026.

BIONI, Bruno; EILBERG, Daniela Dora; CUNHA, Brenda; SALIBA, Pedro; VERGILI, Gabriela. Proteção de dados no campo penal e de segurança pública: nota técnica sobre o Anteprojeto de Lei de Proteção de Dados para segurança pública e investigação criminal. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2020. Disponível em: <<https://www.dataprivacybr.org/wp-content/uploads/2021/11/NT-PROTECAO-DE-DADOS-NO-CAMPO-PENAL-E-DE-SEGURANCA-PUBLICA.pdf>>. Acesso em: 15 jul. 2025.

BOTTINO, Thiago; VARGAS, Daniel; PRATES, Fernanda (coords.). Segurança pública na era do big data: mapeamento e diagnóstico da implementação de novas tecnologias no combate à criminalidade [recurso eletrônico]. Rio de Janeiro: FGV Direito Rio, 2023. Disponível em: <<https://repositorio.fgv.br/server/api/core/bitstreams/869f434b-4ea1-4b73-ae69-983cde99e084/content>>. Acesso em: 15 ago. 2025.

BRASIL. Câmara dos Deputados. PL 1515/2022: ficha de tramitação. Brasília, DF: Câmara dos Deputados, 2022. Disponível em: <<https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2326300#tramitacoes>>. Acesso em: 25 jan. 2026.

BRASIL. Câmara dos Deputados. Projeto de Lei n. 1.515, de 2022. Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais. Autor: Coronel Armando. Brasília, DF: Câmara dos Deputados, 2022. Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2182274&filename=PL%201515/2022>. Acesso em: 20 jan. 2026.

BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, 1988. Disponível em: <https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 25 jan. 2026.

BRASIL. Lei n. 13.675, de 11 de junho de 2018. Disciplina a organização e o funcionamento dos órgãos responsáveis pela segurança pública, nos termos do § 7º do art. 144 da Constituição Federal; cria a Política Nacional de Segurança Pública e Defesa Social (PNSPDS); institui o Sistema Único de Segurança Pública (Susp); altera a Lei Complementar n. 79, de 7 de janeiro de 1994, a Lei n. 10.201, de 14 de fevereiro de 2001, e a Lei n. 11.530, de 24 de outubro de 2007; e revoga dispositivos da Lei n. 12.681, de 4 de julho de 2012. Brasília, DF: Presidência da República, 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13675.htm>. Acesso em: 25 jan. 2026.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 10 jul. 2025.

BRASIL. Lei n. 14.600, de 19 de junho de 2023. Estabelece a organização básica dos órgãos da Presidência da República e dos Ministérios. Brasília, DF: Presidência da República, 2023. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/lei/L14600.htm>. Acesso em: 25 jan. 2026.

BRASIL. Ministério da Justiça e Segurança Pública. Portaria do MJSP regulamenta uso de tecnologia em investigações criminais e inteligência de segurança pública. Gov.br, 30 jun. 2025. Disponível em: <<https://www.gov.br/mj/pt-br/assuntos/noticias/portaria-do-mjsp-regulamenta-uso-de-tecnologia-em-investigacoes-criminais-e-inteligencia-de-seguranca-publica>>. Acesso em: 25 jan. 2026.

BRASIL. Ministério da Justiça e Segurança Pública. Portaria MJSP n. 961, de 24 de junho de 2025. Estabelece diretrizes sobre uso de soluções de tecnologia da informação aplicadas às atividades de investigação criminal e inteligência de segurança pública. Diário Oficial da União: seção 1, Brasília, DF, ed. 120, p. 104, 30 jun. 2025. Disponível em: <<https://www.in.gov.br/web/dou/-/portaria-mjsp-n-961-de-24-de-junho-de-2025-638661609>>. Acesso em: 15 jul. 2025.

BRASIL. Senado Federal. Projeto de Lei n. 2.338, de 2023. Dispõe sobre o uso da Inteligência Artificial. Autor: Senador Rodrigo Pacheco. Brasília, DF: Senado Federal, 2023. Disponível em: <<https://www25.senado.leg.br/web/atividade/materias/-/materia/157233>>. Acesso em: 20 jan. 2026.

BREIER, Ricardo. O risco à defesa técnica e à paridade de armas no processo penal: análise crítica da Portaria MJSP n. 961/2025. Abracrim, seção Artigos, 15 jul. 2025. Disponível em: <<https://web.abracrim.adv.br/o-risco-a-defesa-tecnica-e-a-paridade-de-armas-no-processo-penal-analise-critica-da-portaria-mjsp-no-961-2025/>>. Acesso em: 25 jan. 2026.

CALDEIRA, Rodrigo de Andrade Figaro. Inteligência artificial tem crescido na área de segurança pública. Consultor Jurídico, seção Opinião, 2 jul. 2025. Disponível em: <<https://www.conjur.com.br/2025-jul-02/inteligencia-artificial-e-seguranca-publica-analise-critica-da-portaria-961-2025-do-mjsp/>>. Acesso em: 20 jan. 2026.

CAMARGO, R. O. de. Tratamento de dados, persecução penal e garantia do direito de defesa. 2022. Tese (Doutorado em Direito) — Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2022. Disponível

em: <<https://tede2.pucrs.br/tede2/handle/tede/10605>>. Acesso em: 15 ago. 2025.

CAMPELO, Marcelo. A influência da tecnologia no Direito Penal: desafios e oportunidades. Migalhas, seção Migalhas de Peso, 18 jan. 2025. Disponível em: <<https://www.migalhas.com.br/depeso/422898/a-influencia-da-tecnologia-no-direito-penal-desafios-e-oportunidades>>. Acesso em: 20 jan. 2026.

CÂMARA DOS DEPUTADOS (@camaradosdeputados). O Marco Legal da Inteligência Artificial é uma das prioridades da Câmara dos Deputados em 2026. Instagram, reel, [s.d.]. Disponível em: <<https://www.instagram.com/reel/DTwAnkXAaB8/>>. Acesso em: 25 jan. 2026.

DATA PRIVACY BRASIL. Tabuleiro #115 | Um primeiro passo na regulação do uso de tecnologias na segurança pública. Data Privacy Brasil, 18 jul. 2025. Disponível em: <<https://dataprivacy.com.br/tabuleiro-115-um-primeiro-passo-na-regulacao-do-uso-de-tecnologias-na-seguranca-publica/>>. Acesso em: 20 jan. 2026.

DI PIERO, Mônica Maria Costa. Segurança pública. Revista do Ministério Público, Rio de Janeiro, n. 19, 2004. Disponível em: <https://www.mprj.mp.br/documents/20184/2791465/Monica_Maria_Costa_Di_Piero.pdf>. Acesso em: 10 jul. 2025.

GARCIA, Rafael de Deus. Ministério da Justiça avança na regulação da IA e se antecipa ao Congresso na LGPD penal. JOTA, seção Opinião & Análise, Artigos, 8 jul. 2025. Disponível em: <<https://www.jota.info/opiniao-e-analise/artigos/mjsp-avanca-na-regulacao-da-ia-e-se-antecipa-ao-congresso-na-lgpd-penal>>. Acesso em: 26 jan. 2026.

INSTITUTO CÁTEDRA. O novo marco da investigação criminal: a Portaria MJSP 961/2025 transforma o uso de tecnologia e inteligência artificial no Brasil. Instituto Cátedra, jul. 2025. Disponível em: <<https://idcatedra.com.br/2025/07/o-novo-marco-da-investigacao-criminal-como-a-portaria->

mjsp-no-961-2025-transforma-o-uso-de-tecnologia-e-inteligencia-artificial-no-brasil/>. Acesso em: 15 ago. 2025.

PINHEIRO, Flávio Maria Leite. O papel da tecnologia e da inteligência artificial na segurança pública: desafios e convergências com os direitos fundamentais individuais e sociais. Revista do Ministério Público do Estado do Rio de Janeiro, Rio de Janeiro, n. 94, out./dez. 2024. Disponível em: <https://www.mprj.mp.br/documents/20184/7377608/flavio_maria_leite_pinheiro.pdf/>. Acesso em: 15 jul. 2025.

SANTOS, Bruno Cavalcante Leitão; JÚNIOR, Francisco de Assis de. A Portaria MJSP 961/2025 e os limites constitucionais ao uso da inteligência artificial na segurança pública. Boletim IBCCRIM, São Paulo, v. 33, n. 397, p. 18-21, dez. 2025. DOI: 10.5281/zenodo.17624181. Disponível em: <https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/2180/1538>. Acesso em: 25 jan. 2026.

UNIÃO EUROPEIA. Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que cria regras harmonizadas em matéria de inteligência artificial e que altera os Regulamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e as Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regulamento da Inteligência Artificial). Jornal Oficial da União Europeia, L, 2024/1689, 12 jul. 2024. Disponível em: <<https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32024R1689>>. Acesso em: 25 jan. 2026.

VIEIRA, Andrey Bruno Cavalcante; SANTOS, Hugo Leonardo Rodrigues. Investigação criminal e tecnologias digitais: algumas reflexões sobre o policiamento preditivo e a admissibilidade de provas digitais. Revista Brasileira de Direito Processual Penal, Porto Alegre, v. 11, n. 1, e1072, jan./abr. 2025. DOI: 10.22197/rbdpp.v11i1.1072. Disponível em: <<https://revista.ibraspp.com.br/RBDPP/article/view/1072>>. Acesso em: 15 jul. 2025.

