ReGeo ISSN: 2177-3246

SEGURANÇA JURÍDICA EM ECOSSISTEMAS DIGITAIS: REGULAÇÃO POR PRINCÍPIOS E AUTORREGULAÇÃO SUPERVISIONADA PARA IA E BLOCKCHAIN NO BRASIL

LEGAL SECURITY IN DIGITAL ECOSYSTEMS: REGULATION BY PRINCIPLES AND SUPERVISED SELF-REGULATION FOR AI AND BLOCKCHAIN IN BRAZIL

SEGURIDAD JURÍDICA EN ECOSISTEMAS DIGITALES: REGULACIÓN POR PRINCIPIOS Y AUTORREGULACIÓN SUPERVISADA PARA IA Y BLOCKCHAIN EN BRASIL

10.56238/revgeov17n3-038

Sadre Pantoja Alho
Doutorando em Ciências Jurídicas
Instituição: Universidad del Museo Social Argentino (UMSA)
E-mail: sadrepantoja@gmail.com

RESUMO
Este estudo aborda o dilema de conciliar a segurança jurídica — entendida como previsibilidade normativa e proteção de direitos — com o ritmo acelerado de inovação em inteligência artificial e blockchain. Analisa-se como a regulação baseada em princípios pode conferir flexibilidade, enquanto a autorregulação supervisionada (p.ex., prevista no art. 50 da LGPD) incentiva a participação dos setores na formulação de normas específicas. A pesquisa propõe um modelo híbrido graduado por risco, combinando soft law e hard law, interoperabilidade técnica, mecanismos de transparência auditável, ODR (Resolução de Disputas Online) e instrumentos econômicos (seguros e fundos de compensação) para assegurar eficácia e proteção efetiva em ambientes descentralizados. Aplica-se esse modelo ao caso dos registros públicos, sob a hipótese SIM (Sustentabilidade–Interoperabilidade–Marco regulatório). Como exemplo internacional, examinam-se o MiCA e AI Act na UE, arranjos setoriais nos EUA e iniciativas na Argentina (identidade digital blockchain).

Palavras-chave: Segurança Jurídica. Inteligência Artificial. Blockchain. Regulação por Princípios. Autorregulação. LGPD. Ecossistemas Digitais.

ABSTRACT
This study addresses the dilemma of reconciling legal certainty—understood as normative predictability and protection of rights—with the accelerated pace of innovation in artificial intelligence and blockchain. It analyzes how principle-based regulation can provide flexibility, while supervised self-regulation (e.g., as provided for in Article 50 of the LGPD) encourages sector participation in the formulation of specific norms. The research proposes a risk-graded hybrid model, combining soft law and hard law, technical interoperability, auditable transparency mechanisms, ODR (Online Dispute Resolution), and economic instruments (insurance and compensation funds) to ensure effectiveness and effective protection in decentralized environments. This model is applied to the case of public registries, under the SIM (Sustainability–Interoperability–Regulatory Framework) hypothesis. As an

international example, the MiCA and AI Act in the EU, sectoral arrangements in the USA, and initiatives in Argentina (blockchain digital identity) are examined.

Keywords: Legal Certainty. Artificial Intelligence. Blockchain. Principle-Based Regulation. Self-Regulation. LGPD (Brazilian General Data Protection Law). Digital Ecosystems.

RESUMEN

Este estudio aborda el dilema de conciliar la seguridad jurídica —entendida como previsibilidad normativa y protección de derechos— con el ritmo acelerado de la innovación en inteligencia artificial y blockchain. Analiza cómo la regulación basada en principios puede brindar flexibilidad, mientras que la autorregulación supervisada (p. ej., la prevista en el artículo 50 de la LGPD) fomenta la participación sectorial en la formulación de normas específicas. La investigación propone un modelo híbrido con evaluación de riesgos, que combina derecho indicativo y vinculante, interoperabilidad técnica, mecanismos de transparencia auditables, resolución de disputas en línea (ODR) e instrumentos económicos (seguros y fondos de compensación) para garantizar la eficacia y la protección efectiva en entornos descentralizados. Este modelo se aplica al caso de los registros públicos, bajo la hipótesis SIM (Sostenibilidad-Interoperabilidad-Marco Regulatorio). Como ejemplo internacional, se examinan la Ley de Inteligencia Artificial (MiCA) y la Ley de Inteligencia Artificial en la UE, los acuerdos sectoriales en EE. UU. y las iniciativas en Argentina (identidad digital blockchain).

Palabras clave: Seguridad Jurídica. Inteligencia Artificial. Blockchain. Regulación por Principios. Autorregulación. LGPD (Ley General de Protección de Datos de Brasil). Ecosistemas Digitales.

1 INTRODUÇÃO

Em ambientes digitais emergentes (IA e blockchain) há tensão entre a necessidade de segurança jurídica, ou seja, previsibilidade, coerência e estabilidade nas normas que regulam direitos e responsabilidades e a velocidade das inovações tecnológicas. Enquanto a segurança jurídica favorece decisões com *grau de certeza* quanto às consequências legais, a inovação exige flexibilidade regulatória. Como observa um estudo do poder legislativo, "a experimentação requer previsibilidade e segurança jurídica. Na inovação, espera-se o erro, desde que não seja grosseiro, pois é assim que… novas tecnologias … são desenvolvidas". O desafio é compatibilizar essas forças, evitando zonas cinzentas de incerteza quanto à responsabilidade e jurisdição em sistemas descentralizados sem sufocar o potencial inovador.

O problema central deste trabalho é: como compatibilizar a previsibilidade normativa e a tutela de direitos com a velocidade de inovação em IA e blockchain, reduzindo as áreas de incerteza ("zonas cinzentas") sobre responsabilidade, jurisdição e reparação em ambientes descentralizados? Esse tema tem grande relevância pública, pois a desregulamentação pode minar a confiança dos usuários e investidores, enquanto uma regulação rígida e detalhista pode engessar o desenvolvimento tecnológico.

Em especial, sistemas baseados em blockchain e IA geram desafios inéditos de enforcement: a descentralização dificulta identificar quem é o titular do dever (usuário, desenvolvedor ou plataforma) e qual lei aplicar em casos transfronteiriços. A hipótese de partida é que um modelo regulatório híbrido (princípio + autorregulação supervisionada) graduado por risco pode oferecer um equilíbrio dinâmico, assegurando transparência e meios efetivos de reparação mesmo em cenários de alta inovação.

O objetivo geral é propor um modelo normativo híbrido para IA e blockchain no Brasil, que combine regulação por princípios (normas gerais de alto nível) com autorregulação supervisionada pelos setores afetados, de modo a diferenciar deveres e responsabilidades conforme o risco de cada atividade. Busca-se também estabelecer mecanismos de governança (transparência, ODR, seguros, fundos) que viabilizem execução efetiva dos deveres e reparação de danos. Os objetivos específicos incluem: analisar teorias e exemplos de segurança jurídica, regulação por princípios e autorregulação setorial (p.ex. art. 50 da LGPD); (examinar experiências internacionais relevantes (Europa, EUA, Argentina) em blockchain e IA.

A pesquisa segue abordagem qualitativa e normativa, combinando revisão bibliográfica e documental. Utiliza-se análise de princípios constitucionais (econômicos, processuais e tecnológicos) e doutrina sobre regulação e governança digital. Realiza-se estudo comparativo de legislações e propostas (PLs e regulamentos), além de experiências setoriais (p.ex., sandbox, códigos de conduta). A delimitação recai sobre o contexto brasileiro e internacional recente (até 2025). Conceitos operacionais importantes: ecossistemas digitais (aplicações integradas de IA e blockchain); regulação

por princípios (regulatory principles que orientam, mas não normatizam detalhadamente); autorregulação supervisionada (normas desenvolvidas pelos setores, reconhecidas e fiscalizadas por autoridade pública, conforme LGPD art. 50); segurança jurídica (direito à previsibilidade e estabilidade normativa).

2 FUNDAMENTOS TEÓRICO-NORMATIVOS

2.1 SEGURANÇA JURÍDICA E REGULAÇÃO POR PRINCÍPIOS

A segurança jurídica ocupa posição central na teoria do Estado de Direito e funciona como condição mínima de previsibilidade para qualquer projeto de regulação de ecossistemas digitais. No plano constitucional brasileiro, ela se extrai do conjunto de garantias do artigo 5º da Constituição de 1988 – sobretudo da proteção ao direito adquirido, ao ato jurídico perfeito e à coisa julgada (art. 5º, XXXVI) – bem como dos princípios da legalidade, impessoalidade, moralidade, publicidade e eficiência previstos no artigo 37, caput (Brasil, 1988). Essa base constitucional indica que o Direito deve assegurar um horizonte minimamente estável, compreensível e previsível, de forma a permitir que indivíduos e organizações planejem sua conduta sem serem surpreendidos por mudanças bruscas do ordenamento.

Humberto Ávila desenvolve talvez a formulação mais influente dessa ideia ao tratar da segurança jurídica como princípio estruturante. Em sua *Teoria da segurança jurídica*, o autor distingue uma dimensão estática, ligada à cognoscibilidade do Direito, e uma dimensão dinâmica, conectada à confiabilidade e à calculabilidade das normas (Ávila, 2016). A cognoscibilidade refere-se à exigência de que o ordenamento seja minimamente inteligível, de modo que o cidadão consiga compreender o conteúdo e o alcance dos comandos jurídicos; a confiabilidade volta-se à estabilidade da ordem normativa, evitando que a pessoa tenha frustrada a confiança depositada em um determinado estado de coisas; a calculabilidade, por sua vez, aponta para a necessidade de que mudanças ocorram de forma suave, permitindo projeções razoáveis para o futuro (Ávila, 2016; Valiati, 2015).

Para enfrentar esse tipo de cenário, parcela expressiva da doutrina aponta que modelos rígidos, inteiramente baseados em regras detalhadas, tendem a envelhecer rapidamente e a produzir assimetria informacional ainda maior. A regulação por comandos estritamente casuísticos, dependente de sucessivas alterações legislativas, encontra dificuldade evidente para acompanhar o ritmo da inovação (Freitas, 2016; Moreira Neto, 2005). Daí a crescente atenção conferida à chamada regulação por princípios, em que o núcleo normativo é composto por standards abertos – como transparência, diligência, proporcionalidade, equidade ou accountability algorítmica –, que orientam a atuação de reguladores e agentes econômicos em situações novas, ainda não previstas pelo legislador. Argumentativa por parte das agências reguladoras e dos próprios regulados.

Lacerda (2021), ao analisar modelos contábeis inspirados em princípios, mostra que:

> O uso de standards aumenta o espaço para o julgamento profissional, mas, simultaneamente, reforça a necessidade de transparência das razões e de controles institucionais mais sofisticados. Essa lógica pode ser transposta para o domínio da IA e do blockchain: princípios como explicabilidade, governança de dados e prevenção de danos não esgotam, em si mesmos, o conteúdo da obrigação, porém servem como eixos de orientação obrigatória para reguladores, desenvolvedores e operadores de plataformas.

No debate brasileiro atual, a Agência Nacional do Petróleo e o Governo Federal, em documentos de boas práticas regulatórias, já reconhecem a regulação baseada em princípios como instrumento adequado em setores caracterizados por alta inovação, justamente por permitir adaptação gradual às mudanças tecnológicas, sem abdicar de comandos mínimos e de mecanismos de enforcement (Agência Nacional do Petróleo, 2019; Fonseca & Costa, 2020). Estudos recentes sobre direito regulatório, por sua vez, descrevem esse movimento como transição de um modelo de "comando e controle" para arranjos mais cooperativos e responsivos (Guerra, 2011; Freitas, 2016).

É justamente nesse ponto que entra o conceito de regulação responsiva, desenvolvido originalmente por Ian Ayres e John Braithwaite em *Responsive Regulation: Transcending the Deregulation Debate* (Ayres & Braithwaite, 1995). Os autores propõem uma "pirâmide regulatória" em que instrumentos de persuasão, cooperação e autorregulação ocupam os degraus inferiores, enquanto sanções mais gravosas e comandos rígidos aparecem nos níveis superiores, acionados somente em caso de resistência ou reincidência. A lógica da responsividade consiste em calibrar a reação do Estado conforme o comportamento dos regulados, combinando estímulos, monitoramento e punição graduada, com o objetivo de fortalecer a conformidade voluntária e reduzir custos de supervisão.

No Brasil, esse paradigma começa a ser absorvido em vários setores, inclusive no direito administrativo sancionador de agências reguladoras. Rodrigues (2025) descreve a regulação responsiva como modelo que busca conciliar a flexibilização normativa com a preservação do interesse público, por meio de mecanismos de escuta, cooperação e apenas posterior aplicação de sanções, quando necessário (Rodrigues, 2025).

Esse diálogo entre segurança jurídica, regulação por princípios e regulação responsiva oferece uma chave teórica particularmente útil para ecossistemas digitais. Em vez de um conjunto fechado de regras detalhadas, o que se projeta é um sistema de princípios estruturantes – dignidade da pessoa humana, proteção de dados, livre iniciativa, proteção do consumidor, neutralidade de rede, não discriminação algorítmica, transparência, accountability –, combinados com mecanismos graduais de enforcement. Reguladores estabelecem parâmetros gerais obrigatórios, baseados em risco, enquanto atores privados desenvolvem códigos de conduta, programas de conformidade e arranjos de autorregulação supervisionada, sujeitos a auditorias, supervisão contínua e sanções proporcionais em caso de descumprimento.

No campo específico de IA e blockchain, esse arranjo se mostra compatível com a exigência de previsibilidade normativa sem engessamento tecnológico. Do ponto de vista da segurança jurídica, princípios claros e estáveis – como obrigação de avaliação de impacto de IA, dever de registro de logs imutáveis em redes distribuídas, requisitos de governança e de documentação técnica – permitem que agentes econômicos compreendam antecipadamente os parâmetros de atuação, ainda que a forma concreta de cumprimento varie conforme o modelo de negócio e o grau de risco. A regulação responsiva, por sua vez, oferece o ferramental para graduar deveres e reações conforme o histórico de conformidade, a criticidade da aplicação e o potencial de dano, preservando os ideais de cognoscibilidade, confiabilidade e calculabilidade destacados por Ávila (2016).

2.2 AUTORREGULAÇÃO SUPERVISIONADA (LGPD, ART. 50, E EXPERIÊNCIAS SETORIAIS)

A autorregulação supervisionada (ou corregulação) é instrumento onde setores econômicos elaboram padrões de boas práticas que são reconhecidos por autoridade pública. No Brasil, a LGPD inaugurou essa ideia no art. 50, facultando aos controladores e operadores, isoladamente ou via associações, formular "regras de boas práticas e de governança" relativas ao tratamento de dados

. Essas regras devem detalhar condições organizacionais, procedimentos, segurança, padrões técnicos, supervisão e mitigação de riscos (p.ex., reclamações de titulares, ações educativas)

. O §1º do art. 50 exige que essas regras considerem "natureza, escopo, finalidade, probabilidade e gravidade dos riscos e benefícios" do tratamento, demonstrando foco na proporcionalidade setorial. Uma vez reconhecidas pela ANPD, tais regras são divulgadas como referência para o setor, constituindo espécie de certificado de conformidade.

No debate brasileiro atual, a Agência Nacional do Petróleo e o Governo Federal, em documentos de boas práticas regulatórias, já reconhecem a regulação baseada em princípios como instrumento adequado em setores caracterizados por alta inovação, justamente por permitir adaptação gradual às mudanças tecnológicas, sem abdicar de comandos mínimos e de mecanismos de enforcement (Agência Nacional do Petróleo, 2019; Fonseca & Costa, 2020). Estudos recentes sobre direito regulatório, por sua vez, descrevem esse movimento como transição de um modelo de "comando e controle" para arranjos mais cooperativos e responsivos (Guerra, 2011; Freitas, 2016).

É justamente nesse ponto que entra o conceito de regulação responsiva, desenvolvido originalmente por Ian Ayres e John Braithwaite em *Responsive Regulation: Transcending the Deregulation Debate* (Ayres & Braithwaite, 1995). Os autores propõem uma "pirâmide regulatória" em que instrumentos de persuasão, cooperação e autorregulação ocupam os degraus inferiores, enquanto sanções mais gravosas e comandos rígidos aparecem nos níveis superiores, acionados somente em caso de resistência ou reincidência. A lógica da responsividade consiste em calibrar a reação do Estado conforme o comportamento dos regulados, combinando estímulos, monitoramento e

punição graduada, com o objetivo de fortalecer a conformidade voluntária e reduzir custos de supervisão.

No Brasil, esse paradigma começa a ser absorvido em vários setores, inclusive no direito administrativo sancionador de agências reguladoras. Rodrigues (2025) descreve a regulação responsiva como modelo que busca conciliar a flexibilização normativa com a preservação do interesse público, por meio de mecanismos de escuta, cooperação e apenas posterior aplicação de sanções, quando necessário (Rodrigues, 2025).

Esse diálogo entre segurança jurídica, regulação por princípios e regulação responsiva oferece uma chave teórica particularmente útil para ecossistemas digitais. Em vez de um conjunto fechado de regras detalhadas, o que se projeta é um sistema de princípios estruturantes – dignidade da pessoa humana, proteção de dados, livre iniciativa, proteção do consumidor, neutralidade de rede, não discriminação algorítmica, transparência, accountability –, combinados com mecanismos graduais de enforcement. Reguladores estabelecem parâmetros gerais obrigatórios, baseados em risco, enquanto atores privados desenvolvem códigos de conduta, programas de conformidade e arranjos de autorregulação supervisionada, sujeitos a auditorias, supervisão contínua e sanções proporcionais em caso de descumprimento.

2.3 LAG REGULATÓRIO, HARD/SOFT LAW E COORDENAÇÃO INSTITUCIONAL NO BRASIL

O conceito de lag regulatório refere-se ao descompasso entre o ritmo de inovação e a capacidade de criação de normas estatais. No mundo digital, produtos e serviços evoluem mais rápido que leis específicas. Para contornar esse descompasso, adotam-se instrumentos de *soft law* (diretrizes, guias, normas técnicas voluntárias) e abordagens responsivas. No Brasil, observa-se tendência em priorizar normas gerais e avaliação de impacto ao legislar inovações. O Estado estimula a regulação experimental (ex. decreto de sandbox financeiro/tecnológico, autorregulação cooperada) justamente por reconhecer que “medidas regulatórias sem aprovação legislativa devem ser preferidas, dado seu potencial de responsividade célebre”. Em outras palavras, ante o lag, prefere-se delegar poderes (via agências, acordos cooperativos e resoluções administrativas) a permitir sandbox ou códigos setoriais.

Essa estratégia implica coordenação institucional entre órgãos envolvidos. Por exemplo, a ANPD tem firmado acordos de cooperação técnica com a Senacon, CADE, NIC.br e TSE para alinhar proteção de dados com concorrência e internet aberta. Já o CNJ e o CNMP dialogam em iniciativas de IA judicial, e outras agências reguladoras (SUSEP em fintechs, ANATEL em IoT) desenvolvem regras setoriais específicas. Entretanto, o Brasil ainda carece de um órgão central integrado de governança digital. O Judiciário, por sua vez, lida com litígios emergentes sem padrão único, o que reforça a necessidade de diretrizes coerentes. Nesse panorama, distingue-se hard law (leis, decretos, resoluções)

de soft law (códigos de conduta, recomendações, certificações). O uso estratégico de soft law pode acelerar respostas sem abrir mão da regulação quando necessário. A participação social e a transparência (audiências públicas, consulta pública) são cruciais para legitimar essa flexibilização normativa.

2.4 JURISDIÇÃO, RESPONSABILIDADE E REPARAÇÃO EM AMBIENTES DESCENTRALIZADOS

Werbach (2018) descreve a blockchain como nova arquitetura de confiança, na qual os participantes passam a confiar no sistema distribuído e em seus mecanismos de consenso, sem depender da confiabilidade de um intermediário específico.

Essa forma de organização, baseada em imutabilidade relativa, transparência e automação de execuções, reconfigura pontos de contato entre fato e direito: o "local" da transação deixa de corresponder a um território físico, e a própria definição de quem "age" passa a envolver desenvolvedores de protocolos, operadores de infraestrutura, emissores de tokens, provedores de carteiras, plataformas de acesso (front-ends) e usuários finais. De Filippi e Wright (2018) denominam esse ambiente de *rule of code*, indicando que o conjunto de regras inscrito na blockchain pode formar uma espécie de "lex cryptographica", ainda submetida, contudo, aos ordenamentos estatais que continuam a prover sanção, coerção legítima e estruturas de reparação.

No plano da jurisdição, a Lei de Introdução às Normas do Direito Brasileiro (LINDB) já orienta a solução de conflitos no tempo e no espaço, funcionando como estatuto de direito internacional privado, com critérios como domicílio das partes, local da constituição da obrigação, local da ocorrência do dano e local da prestação (artigos 7º, 9º e 12).

Em ambientes descentralizados, esses elementos se tornam difusos: o contrato inteligente pode ser programado em um país, executado em nós distribuídos globalmente, vincular partes residentes em diferentes jurisdições e produzir efeitos econômicos em mercados de terceiros Estados. Finck (2019), ao examinar a regulação e a governança de blockchain na Europa, sublinha que a descentralização tende a fragmentar os pontos tradicionais de conexão, o que exige foco renovado em atores que "ancoram" a rede no plano físico, como exchanges, operadores de nós corporativos e provedores de interfaces de usuário.

De Filippi e Wright (2018) destacam que muitos projetos de blockchain tentaram apresentar-se como "fora do alcance" de qualquer autoridade nacional, o que levou a experiências dramáticas, como o colapso do *The DAO*, que revelou limites da auto-organização puramente algorítmica.

Werbach (2017; 2018) argumenta que:

> Blockchain e direito são, ambos, mecanismos de confiança; redes que ignoram a incidência de normas estatais terminam, em algum momento, dependendo de cortes, reguladores ou mecanismos tradicionais de enforcement para corrigir bugs, fraudes ou desequilíbrios contratuais. Em consequência, a dificuldade não reside em suposta "ausência de jurisdição", mas em identificar quais Estados têm conexão suficiente com o litígio e sobre quais atores recairão decisões sobre responsabilidade e reparação.

No contexto brasileiro, o Marco Civil da Internet (Lei nº 12.965/2014) já enfrentou parte dessas questões no âmbito das plataformas centralizadas, ao disciplinar responsabilidade de provedores de conexão e de aplicações por atos de terceiros (arts. 18 a 21), bem como ao exigir que provedores com atividade no país observem a legislação brasileira e cumpram ordens judiciais, ainda que sediados no exterior (art. 11). Debates recentes sobre a constitucionalidade parcial do art. 19, que condicionava responsabilidade à existência de ordem judicial prévia, mostram que modelos exageradamente protetivos em relação aos intermediários podem gerar déficits de tutela de direitos fundamentais. A discussão ainda se move em torno de plataformas como redes sociais e serviços de hospedagem, mas a lógica de gradação de responsabilidade em função do controle sobre o conteúdo, do proveito econômico e da capacidade de prevenir danos oferece parâmetros úteis para ambientes em que smart contracts e registros distribuídos estruturam a prestação de serviços.

A experiência brasileira com responsabilidade de provedores de aplicação em plataformas centralizadas oferece lições relevantes. Estudos de Micheletti (2023) e Pereira (2022) mostram que o desenho original do art. 19 do Marco Civil funcionou como válvula de contenção da responsabilidade, ao exigir ordem judicial específica para que se formasse o dever de remoção e, em consequência, a responsabilidade por danos decorrentes de conteúdo de terceiros.

A evolução legal que vem relativizando essa blindagem em situações de grave violação de direitos fundamentais, indica tendência de aproximação entre responsabilidade de plataformas digitais e deveres de cuidado ampliados em proteção de bens como dignidade, igualdade e integridade psicofísica. Esse movimento sinaliza que, em contextos de IA e blockchain, dificilmente se aceitará narrativa que apresente a descentralização como mecanismo absoluto de exclusão de responsabilidade, sobretudo quando há assimetria informacional e técnica em desfavor do usuário.

3 COMPARAÇÃO INTERNACIONAL

3.1 UNIÃO EUROPEIA: MICA E AI ACT (CRONOGRAMA E OBRIGAÇÕES POR RISCO)

A União Europeia consolidou, nos últimos anos, um bloco normativo voltado a ecossistemas digitais que combina proteção de direitos fundamentais, estabilidade financeira e estímulo à inovação. No campo cripto, o Regulamento (UE) 2023/1114, conhecido como Markets in Crypto-Assets (MiCA), criou um quadro uniforme para criptoativos que não estavam abrangidos por normas financeiras anteriores, com foco em emissores e prestadores de serviços de criptoativos (*crypto-asset service*

providers – CASPs) (European Securities and Markets Authority [ESMA], 2024; European Central Bank, 2023).

O MiCA estrutura o mercado em categorias, como *asset-referenced tokens* (ARTs), *e-money tokens* (EMTs) e outros criptoativos, estabelecendo exigências de autorização, transparência, governança e regras prudenciais proporcionais à natureza do ativo e ao risco sistêmico associado (Hogan Lovells, 2025; Central Bank of Ireland, 2024). Em emissores de stablecoins com lastro em moeda ou cestas de ativos, o regulamento impõe requisitos de reservas, políticas de gestão de liquidez, regras de divulgação e limites de volume, visando reduzir riscos de corrida e contágio financeiro (Cyfrin, 2025; AMF, 2024).

O cronograma de aplicação reforça a lógica gradual e baseada em risco. O texto entrou em vigor em junho de 2023, com as normas sobre ARTs e EMTs passando a valer em 30 de junho de 2024, e o restante do regime – especialmente as obrigações dos CASPs – aplicável a partir de 30 de dezembro de 2024 (Cyfrin, 2025; ESMA, 2024).

Estados-membros podem conceder período de transição de até 18 meses para prestadores já ativos, o que cria uma espécie de "rampa regulatória" que tenta conciliar segurança jurídica e não interrupção brusca de serviços (Squire Patton Boggs, 2025).

Outro ponto relevante do MiCA está no mecanismo de *passporting*: uma vez autorizado em um Estado-membro, o CASP pode prestar serviços em todo o mercado único, mediante notificações e cooperação entre autoridades nacionais (Central Bank of Ireland, 2024; Hogan Lovells, 2025).

Essa estrutura reduz custos de múltiplas licenças, mas exige coordenação regulatória intensa, com diretrizes comuns de supervisão e canais de troca de informações. Em termos de segurança jurídica, o efeito principal é converter um mosaico de regimes nacionais em um conjunto homogêneo de obrigações mínimas, que passam a valer para todo o ecossistema europeu de criptoativos.

No domínio da inteligência artificial, a União Europeia aprovou o AI Act, descrito pelas próprias instituições europeias como o primeiro marco normativo abrangente voltado a sistemas de IA. O regulamento adota abordagem claramente baseada em risco, com proibição de determinadas práticas (como sistemas de *social scoring* e vigilância biométrica massiva em tempo real) e um regime rigoroso para sistemas de "alto risco", que precisam cumprir exigências de governança, documentação, gestão de risco, qualidade de dados e supervisão humana (European Commission, 2025; European Parliamentary Research Service, 2025).

O cronograma de implementação é escalonado. As proibições passaram a valer em fevereiro de 2025; a partir de agosto de 2025 surgem obrigações específicas para modelos de propósito geral; e, em agosto de 2026, inicia-se a aplicação do regime completo para sistemas de alto risco, com prazo estendido para sistemas legados até 2027 (European Parliamentary Research Service, 2025; Trilateral Research, 2025; Reuters, 2025).

O regulamento exige ainda que cada Estado-membro crie ao menos um *sandbox* regulatório de IA até agosto de 2026, com o objetivo de testar soluções em ambiente controlado e sob supervisão das autoridades competentes (AIAct.eu, 2025).

A literatura destaca que tanto o MiCA quanto o AI Act ilustram um estilo de regulação em que o legislador europeu tenta antecipar riscos e estabelecer um quadro horizontal que depois será concretizado por guias, normas técnicas e decisões das autoridades setoriais (Finck, 2019; Sartor, 2020). Em termos de segurança jurídica, esse modelo tende a produzir previsibilidade maior sobre critérios de licenciamento, classificação de risco, deveres de diligência e possibilidades de responsabilização, ainda que crie custos regulatórios expressivos.

Outra característica que interessa diretamente ao TCC é a conexão entre regulação baseada em risco e mecanismos de reparação. No AI Act, há previsão de documentação robusta, registros de eventos e rastreabilidade, que facilitam a prova em litígios envolvendo danos causados por sistemas de IA (European Commission, 2025; European Parliament, 2025).

No MiCA, os CASPs precisam dispor de mecanismos de tratamento de reclamações, políticas de gestão de conflitos de interesse e procedimentos para tratamento de incidentes de segurança, o que abre espaço para integração com ODR e seguros de responsabilidade (ESMA, 2024; AMF, 2024).

3.2 ESTADOS UNIDOS: ARRANJO MULTÍNGREME DE AGÊNCIAS (SÍNTESE FUNCIONAL)

O caso norte-americano segue lógica quase oposta à europeia. Em vez de um regulamento único para IA ou criptoativos, o país opera com um conjunto disperso de normas setoriais, orientações administrativas, *guidelines* técnicos e enforcement por múltiplas agências. A pesquisa do Congressional Research Service registra que, até meados de 2025, não havia legislação federal ampla sobre IA, predominando leis pontuais e políticas administrativas, com foco em segurança nacional, defesa, privacidade em setores específicos e consumo (Congressional Research Service, 2025).

No campo da IA, o governo federal vem apostando em instrumentos de *soft law*. O National Institute of Standards and Technology (NIST) publicou, em 2023, o AI Risk Management Framework, concebido como guia voluntário para organizações que desejam estruturar governança de risco em IA, com ênfase em confiabilidade, transparência, equidade e mitigação de vieses (NIST, 2023).

Em 2023, foi editada ordem executiva sobre desenvolvimento “seguro e confiável” de IA, seguida pelo *America’s AI Action Plan* de 2025, que estabelece metas de política pública e atribui tarefas a órgãos como o NIST, o Departamento de Comércio, a Federal Trade Commission (FTC) e o Department of Justice (DOJ) (White House, 2023; White House, 2025).

A literatura descreve essa arquitetura como modelo descentralizado, baseado em agências independentes, com forte uso de orientações técnicas e enforcement ex post. Davtyan (2025) analisa que a abordagem norte-americana se apoia em uma combinação de compromissos voluntários de

empresas, *guidelines* de órgãos como NIST, FTC e FDA, e atuação repressiva do DOJ em casos de uso abusivo de IA, sem um quadro único comparável ao AI Act (Davtyan, 2025; Associated Press, 2024).

No plano dos criptoativos, a fragmentação se torna ainda mais evidente. O mercado é supervisionado por um conjunto de órgãos que inclui a Securities and Exchange Commission (SEC), a Commodity Futures Trading Commission (CFTC), o Departamento do Tesouro (via FinCEN e OFAC), os reguladores bancários federais (Federal Reserve, OCC, FDIC), além de órgãos estaduais responsáveis por licenças de transmissão de valores e proteção ao consumidor (Latham & Watkins, 2025; Holland & Knight, 2025).

A SEC, em geral, enquadra determinados criptoativos como valores mobiliários, com base no teste de *investment contract* derivado de *SEC v. Howey Co.*, e supervisiona ofertas públicas, exchanges e *tokens* que se enquadrem como valores mobiliários (Merkle Science, 2024; SEC, 2025).

A CFTC trata criptoativos como commodities nos mercados de derivativos, com competência sobre contratos futuros, *swaps* e mercados de margem, além de fiscalizar manipulação e fraude (CFTC, 2025; WilmerHale, 2025).

Relatório recente sobre o quadro regulatório de blockchain e cripto nos EUA descreve esse arranjo como sobreposição dinâmica: SEC e CFTC disputam espaços de competência, enquanto FinCEN aplica normas de prevenção à lavagem de dinheiro e OFAC controla sanções, gerando cenário em que a mesma plataforma pode estar sujeita a múltiplas cadeias de obrigações, muitas vezes com divergências interpretativas (Holland & Knight, 2025).

No campo da responsabilidade, a ausência de um marco único faz com que princípios tradicionais de *securities law*, proteção ao consumidor e responsabilidade civil se projetem sobre casos envolvendo IA e criptoativos. A FTC vem sinalizando que práticas enganosas associadas à IA – por exemplo, alegações infundadas sobre capacidades de sistemas – podem ser enquadradas como *unfair or deceptive acts or practices*, enquanto o DOJ já anunciou que o uso de IA para intensificar crimes de colarinho branco pode agravar penas (Department of Justice, 2024).

No plano federativo, iniciativas estaduais de regulação de IA e cripto são crescentes, o que levou a discussões sobre eventual ordem executiva para limitar leis estaduais consideradas excessivamente restritivas (Politico, 2025).

Sob a ótica da segurança jurídica, esse arranjo multíngreme produz ambiguidade importante. Há elevada capacidade de reação por parte de agências, que podem emitir orientações rápidas e atuar em enforcement, mas os agentes econômicos lidam com incerteza sobre a qualificação jurídica de ativos, a fronteira entre competência da SEC e da CFTC, a incidência de regras estaduais e a possibilidade de mudanças de orientação conforme a Administração em exercício (Wired, 2025; Latham & Watkins, 2025). Ao mesmo tempo, esse modelo revela instrumentos úteis de coordenação

interagências e uso intensivo de normas técnicas e *guidelines* que podem inspirar arranjos responsivos no contexto brasileiro.

3.3 ARGENTINA: DIGITALIZAÇÃO REGISTRAL, IDENTIDADE/ASSINATURA DIGITAL E INICIATIVAS EM IA/BLOCKCHAIN

A experiência argentina oferece um exemplo de país latino-americano que consolidou, relativamente cedo, uma base jurídica para documentos e assinaturas digitais e, progressivamente, vem incorporando tecnologias de registro distribuído em políticas de governo digital e em iniciativas setoriais. A Lei n.º 25.506, de 2001, instituiu o regime de firma digital e firma eletrônica, reconhecendo eficácia jurídica a documentos eletrônicos assinados digitalmente e criando a Infraestructura de Firma Digital da República Argentina (IFDRA) (Argentina, 2001; Argentina.gob.ar, 2016).

Normas posteriores, como a Lei 27.446 e decretos regulamentares, atualizaram esse marco, integrando a firma digital à gestão documental eletrônica da Administração Pública e incentivando sua utilização em contratos, petições administrativas e atos registrais (Argentina.gob.ar, 2016; Ecertla, 2023).

A doutrina ressalta que esse arranjo conferiu à assinatura digital estatuto equivalente ao da assinatura manuscrita, desde que respeitados requisitos de certificação e integridade, o que permitiu a expansão de serviços jurídicos digitais, como despachos eletrônicos e trâmites notariais à distância (CheersContracts, 2025).

No campo da digitalização registral, diversos projetos exploram a utilização de blockchain como camada adicional de confiabilidade. Estudo de Pagella (2022) analisa a aplicação de blockchain no Registro da Propriedade Imobiliária da Capital Federal, avaliando ganhos potenciais em autenticidade, imutabilidade e rastreabilidade dos atos registrais (Pagella, 2022).

A mesma linha aparece em projetos como o Registro Público de Graduados Universitários, cuja base de dados, vinculada ao Ministério da Educação, passou a utilizar blockchain para autenticar diplomas e históricos acadêmicos, permitindo que terceiros verifiquem a veracidade das informações de forma pública e auditável (Blockchain Federal Argentina, s.d.).

Há, ainda, iniciativas normativas regionais que mencionam explicitamente registros distribuídos. O Plano de Transformação Pública Digital da província de Santa Cruz, por exemplo, autoriza o Executivo a empregar tecnologias de registros distribuídos e redes blockchain, públicas ou privadas, em serviços de governo digital, teletrabalho e processos administrativos, com vistas a aumentar transparência e confiança (Santa Cruz, 2022).Saij Petições públicas encaminhadas a autoridades nacionais solicitam a incorporação de blockchain em registros públicos com o argumento de que a tecnologia poderia reduzir corrupção, fraudes e demora em procedimentos registrais (Change.org, 2025).

O caso mais visível no debate internacional, contudo, é o projeto de identidade digital descentralizada da cidade de Buenos Aires. Em 2024, a capital lançou o sistema QuarkID, integrado ao aplicativo miBA, com a proposta de oferecer credenciais digitais baseadas em blockchain, apoiadas em provas de conhecimento zero (*zero-knowledge proofs*), que permitem aos cidadãos demonstrarem atributos (como idade ou status educacional) com mínima exposição de dados pessoais (Borak, 2024; Coindesk, 2024; ZKsync, 2024).

Relatos oficiais indicam que o projeto pretende alcançar cerca de 3,6 milhões de residentes, configurando a primeira iniciativa de identidade descentralizada habilitada por um governo municipal em escala dessa magnitude (Dig.watch, 2024; ZKsync, 2024).

A lógica subjacente ao QuarkID associa-se à ideia de identidade auto-soberana (*self-sovereign identity – SSI*), em que o titular mantém controle sobre suas credenciais, que podem ser verificadas por terceiros sem necessidade de reter dados em grandes bases centralizadas. Do ponto de vista da segurança jurídica, essa experiência evidencia um esforço de reconciliação entre direitos fundamentais de privacidade, autenticação robusta e exigências de integridade dos registros. A escolha por protocolos com provas de conhecimento zero indica preocupação explícita com proporcionalidade na exposição de dados e com a possibilidade de auditoria técnica sobre os mecanismos de validação (Portaldobitcoin, 2024; Chainwire, 2024; BrazilCrypto, 2024).

É possível observar, ainda, que o avanço da digitalização registral e dos projetos de identidade digital na Argentina ocorre em diálogo com o marco de firma digital e com a infraestrutura de certificação já existente. A interpretação dominante mantém a ideia de que documentos eletrônicos assinados com certificado válido gozam de presunção de autenticidade e integridade, o que facilita a integração entre registros tradicionais e soluções baseadas em blockchain e IA, usadas como camadas adicionais de prova ou de automação de verificações (Argentina.gob.ar, 2016; CheersContracts, 2025).

Em conjunto, esses elementos compõem um cenário em que a Argentina combina, de um lado, base jurídica relativamente consolidada em matéria de documentos e assinaturas digitais; de outro, pilotos experimentais em identidade descentralizada e uso de blockchain em registros públicos, ainda em fase de amadurecimento, mas relevantes como laboratório normativo para a região.

3.4 SÍNTESE COMPARADA E LIÇÕES PARA O BRASIL

A comparação entre União Europeia, Estados Unidos e Argentina revela três caminhos distintos de enfrentamento dos riscos jurídicos associados a IA, criptoativos e registros distribuídos. O modelo europeu, representado pelo MiCA e pelo AI Act, privilegia regulações horizontais e detalhadas, ancoradas em abordagem de risco e combinadas com cronogramas claros, sandboxes regulatórios e mecanismos estruturados de supervisão. A consequência principal é alto grau de previsibilidade quanto

às categorias de risco, aos requisitos de autorização e às possíveis sanções, com custo regulatório elevado e forte centralidade das autoridades europeias.

O arranjo norte-americano, por sua vez, apoia-se em uma rede de agências com competências sobre fragmentos do ecossistema digital. A ausência de um AI Act ou de um MiCA federal faz com que normas de *securities law*, direito do consumidor, combate à lavagem de dinheiro, concorrência e proteção de dados se projetem sobre IA e blockchain de forma casuística, complementadas por *guidelines* técnicos como o NIST AI RMF e por ordens executivas (NIST, 2023; Davtyan, 2025; Congressional Research Service, 2025).

Esse quadro reforça a flexibilidade, mas amplia a incerteza quanto ao futuro das interpretações e à repartição de competência entre órgãos como SEC, CFTC, FTC, FinCEN e reguladores estaduais (Latham & Watkins, 2025; Holland & Knight, 2025).

A experiência argentina ocupa posição intermédia. O país consolidou, com a Lei 25.506 e atualizações, um regime de firma digital e documentos eletrônicos relativamente coeso, que serve de base para digitalização de serviços, processos administrativos e registros. A partir dessa base, surgem projetos de uso de blockchain em registros de propriedade e diplomas, bem como a iniciativa QuarkID em Buenos Aires, com identidade digital descentralizada apoiada em provas de conhecimento zero (Pagella, 2022; Blockchain Federal Argentina, s.d.; Dig.watch, 2024; ZKsync, 2024).

Para o debate brasileiro sobre segurança jurídica em ecossistemas digitais, essas três experiências geram algumas lições centrais, diretamente relacionadas à hipótese de um modelo híbrido baseado em regulação por princípios e autorregulação supervisionada:

> Graduação de deveres por risco, como no AI Act e no MiCA, mostra-se compatível com a ideia de modular obrigações ao longo das camadas de protocolo, infraestrutura, aplicação e intermediação, inclusive no contexto de registros públicos e de IA aplicada a serviços notariais e registrais.
> Passaportização e reconhecimento mútuo de programas de conformidade, típicos do MiCA, apontam caminho para que códigos de conduta e programas de governança em IA e blockchain no Brasil sejam reconhecidos por autoridades setoriais, com efeitos em diferentes mercados, reduzindo custos de múltiplas autorizações.
> Coordenação interagências, ainda que desigual no modelo norte-americano, fornece exemplos de mecanismos de articulação entre órgãos financeiros, de defesa do consumidor, de proteção de dados e de concorrência, aspecto relevante diante da sobreposição entre Banco Central, CVM, Cade, ANPD e Judiciário no tema IA/blockchain.
> Ancoragem em marcos de identidade e assinatura digitais, como se observa na Argentina, indica que qualquer desenho de ecossistema registral baseado em blockchain precisa dialogar com a infraestrutura já existente de ICP-Brasil, certificação digital, assinaturas avançadas e novos modelos de identificação, inclusive soluções descentralizadas compatíveis com direitos de proteção de dados (ZKsync, 2024).

Sob essa perspectiva, a comparação internacional reforça a plausibilidade da hipótese SIM (Sustentabilidade–Interoperabilidade–Marco regulatório) aplicada aos registros públicos brasileiros.

A sustentabilidade institucional das serventias, a interoperabilidade técnico-normativa e a construção de um marco regulatório que combine princípios claros, autorregulação supervisionada e

instrumentos eficazes de execução e reparação encontram, na experiência europeia, norte-americana e argentina.

4 CONCLUSÃO

Em síntese, o artigo partiu da constatação de que a expansão de ecossistemas digitais baseados em inteligência artificial e blockchain intensifica um dilema clássico do Estado de Direito: de um lado, a exigência de segurança jurídica, traduzida em previsibilidade, estabilidade mínima e possibilidade de cálculo quanto às consequências jurídicas das condutas; de outro, a necessidade de abertura normativa suficiente para não asfixiar processos de inovação que se desenvolvem em ciclos muito mais rápidos do que o tempo legislativo. A pergunta inicial — como compatibilizar previsibilidade normativa e tutela de direitos com a velocidade de inovação em ambientes descentralizados — orientou a análise dos fundamentos constitucionais, dos modelos regulatórios e das experiências estrangeiras, permitindo propor um caminho intermediário entre desregulação e excesso de detalhamento legal.

A reconstrução da segurança jurídica como princípio estruturante evidenciou que ela não se reduz à conservação literal de normas, mas envolve cognoscibilidade, confiabilidade e possibilidade de planejamento. A partir daí, o trabalho indicou que um modelo estritamente baseado em regras rígidas, casuísticas e frequentemente alteradas tende a agravar a incerteza em contextos tecnológicos complexos, pois gera sucessivas “camadas” de regulamentação incapazes de acompanhar a realidade. Em contrapartida, a regulação por princípios e a regulação responsiva surgem como alternativas mais adequadas para ecossistemas digitais: princípios como transparência, prevenção, proporcionalidade e governança de dados funcionam como eixos normativos estáveis, enquanto a responsividade permite calibrar a atuação estatal conforme o risco da atividade e o comportamento dos agentes.

No interior desse quadro, a autorregulação supervisionada ganhou relevo especial. A experiência recente de proteção de dados, com códigos de conduta e programas de governança reconhecidos por autoridade especializada, mostra que setores econômicos e órgãos públicos podem assumir responsabilidade na concretização de standards, desde que permaneçam submetidos a parâmetros constitucionais e legais. Em vez de um Estado que tenta antecipar, sozinho, todas as soluções técnicas, desenha-se uma dinâmica em que reguladores definem objetivos, princípios e balizas de risco, enquanto os sujeitos regulados detalham padrões operacionais em diálogo com essas balizas, sob monitoramento, auditoria e possibilidade real de sanção. Tal arranjo demonstra potencial para lidar com tecnologias em rápida mutação, sem abdicar de controle público nem de canais de responsabilização e reparação.

A análise de jurisdição, responsabilidade e reparação em ambientes descentralizados evidenciou que a narrativa de “ausência de lei” em blockchain e IA distribuída não se sustenta. A descentralização complica o mapeamento de quem age, onde age e com qual lei se vincula, mas não

elimina a presença de atores identificáveis que concebem protocolos, mantêm infraestruturas, operam interfaces e exploram economicamente serviços digitais. A conclusão que se impõe é que a segurança jurídica nesses ecossistemas depende da construção de uma rede de responsabilidades graduadas, distribuídas pelas camadas de protocolo, infraestrutura, aplicação, intermediação e uso, com deveres mais intensos para quem detém maior capacidade técnica e econômica de prevenir danos, sem excluir, por completo, a corresponsabilidade de usuários quando atuam de forma dolosa ou em contrariedade manifesta às regras estabelecidas.

O exame comparado de União Europeia, Estados Unidos e Argentina reforçou essa percepção. O modelo europeu, com regulamentos abrangentes e abordagem baseada em risco, mostra que é possível estabelecer categorias claras, cronogramas de implementação e sandboxes obrigatórios, gerando alto grau de previsibilidade, ainda que ao custo de maior densidade normativa. O arranjo norte-americano, mais fragmentado e assentado em múltiplas agências e instrumentos de soft law, revela grande capacidade de reação e adaptação, mas também significativa incerteza quanto à repartição de competências e ao futuro das interpretações. A experiência argentina, ao consolidar um regime de documentos e assinaturas digitais e a partir dele experimentar aplicações de blockchain em registros e identidade digital, evidencia a importância de uma base jurídica bem definida para que projetos inovadores encontrem ancoragem institucional e probatória.

Quando esse conjunto de elementos é projetado sobre o universo dos registros públicos brasileiros, ganha consistência a hipótese de um modelo híbrido pautado pela tríade Sustentabilidade–Interoperabilidade–Marco regulatório. Sustentabilidade diz respeito à viabilidade econômica e institucional das serventias diante da digitalização intensiva, incluindo investimentos em infraestrutura tecnológica, segurança da informação e capacitação de equipes. Interoperabilidade envolve a construção de soluções técnicas e normativas que permitam que registros distribuídos, metadados, APIs e sistemas de IA conversem com a legislação registral, com o processo civil, com a infraestrutura de chaves públicas e com a proteção de dados pessoais, de modo a garantir admissibilidade probatória, rastreabilidade e auditabilidade. Já o componente de marco regulatório remete à necessidade de explicitar, em normas gerais e em instrumentos de autorregulação supervisionada, quem responde por quais riscos em cada camada do ecossistema registral digital, com instrumentos concretos de tutela, como ODR, seguros e fundos de compensação.

Desse percurso decorre uma conclusão central: a segurança jurídica em ecossistemas digitais não exige a paralisação da inovação, mas sim a construção de um ambiente em que inovações relevantes sejam desenvolvidas dentro de um quadro minimamente estável de princípios, deveres e consequências. Um modelo híbrido, baseado em regulação por princípios, regulação responsiva e autorregulação supervisionada, com graduação de deveres por risco e aplicação setorial aos registros públicos sob a hipótese SIM, mostra-se capaz de reduzir zonas cinzentas de responsabilidade,

jurisdição e reparação em ambientes descentralizados, sem sufocar a experimentação tecnológica. Permanecem em aberto, como agenda futura, a necessidade de aprofundar a aplicação prática dessas diretrizes em projetos-piloto, medir empiricamente seus efeitos em termos de eficiência, confiança e redução de litígios e ajustar, a partir desses resultados, a matriz de governança proposta. O ponto de chegada deste artigo, portanto, é a afirmação de que o desafio colocado por IA e blockchain ao Direito brasileiro não é meramente tecnológico, mas institucional e hermenêutico, e que sua resposta mais promissora passa por uma combinação equilibrada de princípios claros, cooperação regulatória e responsabilidade compartilhada.

REFERÊNCIAS

Affonso, G. B. (2023). A responsabilidade civil objetiva pelos danos causados por sistemas de inteligência artificial. *Raízes no Direito*, 9(2).

Agência Europeia de Valores Mobiliários. (2024). *Markets in Crypto-Assets Regulation (MiCA).* Recuperado de https://www.esma.europa.eu

Agência Nacional de Proteção de Dados. (2023). *Relatórios e estudos sobre modelos de fiscalização e regulação responsiva.* Brasília: ANPD.

Agência Nacional do Petróleo. (2019). *Manual de boas práticas regulatórias.* Brasília: ANP.

AIAct.eu. (2025). *AI regulatory sandbox approaches: EU Member State overview.* Recuperado de https://artificialintelligenceact.eu

Almeida, B. S. C. (2020). Aplicabilidade dos smart contracts nas instituições financeiras. *Revista do Banco Central do Brasil*, 16(2).

Argentina. (2001). *Ley 25.506 – Ley de Firma Digital.* Recuperado de https://servicios.infoleg.gob.ar

Argentina.gob.ar. (2016). *Normativa de firma digital.* Recuperado de https://www.argentina.gob.ar

Ávila, H. (2016). *Teoria da segurança jurídica* (4. ed.). São Paulo: Malheiros.

Ávila, H. (2021). *Teoria da segurança jurídica* (6. ed., rev., atual. e ampl.). Salvador: JusPodivm/Malheiros.

Ávila, H. (2025). *Teoria dos princípios: da definição à aplicação dos princípios jurídicos* (nova ed.). Salvador: JusPodivm.

Ayres, I., & Braithwaite, J. (1995). *Responsive regulation: Transcending the deregulation debate.* New York: Oxford University Press.

Barbosa, M. M. (2019). Blockchain e responsabilidade civil: inquietações em torno de uma realidade nova. *Revista de Direito e Responsabilidade.*

Barroso, L. R. (2003). Agências reguladoras: Constituição, transformações do Estado e legitimidade democrática. In D. F. Moreira Neto (Org.), *Direito regulatório*. Rio de Janeiro: Renovar.

Blockchain Federal Argentina. (s.d.). *Registro Público de Graduados Universitarios.* Recuperado de https://bfa.ar

Borak, M. (2024, 23 outubro). Buenos Aires moves from centralized to decentralized digital identity with QuarkID. *Biometric Update.* Recuperado de https://www.biometricupdate.com

Brasil. (1988). *Constituição da República Federativa do Brasil de 1988.* Brasília: Presidência da República.

BrazilCrypto. (2024, 31 outubro). *Latam Crypto Report #19 – Buenos Aires rolls out decentralized identity.* Recuperado de https://newsletter.brazilcrypto.io

Central Bank of Ireland. (2024). *Markets in Crypto-Assets Regulation (MiCAR).* Recuperado de https://www.centralbank.ie

Change.org. (2025). *Incorporar blockchain en la gestión de registros públicos.* Recuperado de https://www.change.org

CheersContracts. (2025, 4 novembro). *Validez jurídica de la firma electrónica en contratos y pagarés en Argentina.* Recuperado de https://www.cheerscontracts.com

Coindesk. (2024, 22 outubro). Buenos Aires adds ZK proofs to city app in bid to boost residents' privacy. Recuperado de https://www.coindesk.com

Congressional Research Service. (2025). *Regulating artificial intelligence: U.S. and international approaches (R48555).* Recuperado de https://www.congress.gov

Cunha, V. (2019). A segurança jurídica e sua natureza de sobreprincípio. *Migalhas de Peso.*

Cyfrin. (2025). *MiCA regulation explained: A guide to EU crypto compliance.* Recuperado de https://www.cyfrin.io

Davtyan, T. (2025). The U.S. approach to AI regulation: Federal laws, policies, and proposals. *Journal of Law, Technology & the Internet*, 16(1). Recuperado de https://scholarlycommons.law.case.edu

Dig.watch. (2024, 24 outubro). Buenos Aires introduces pioneering blockchain-based digital identity for 3.6 million residents. Recuperado de https://dig.watch

European Commission. (2025). *AI Act – European approach to artificial intelligence.* Recuperado de https://digital-strategy.ec.europa.eu

European Parliamentary Research Service. (2025). *AI Act implementation timeline (PE 772.906).* Recuperado de https://www.europarl.europa.eu

Freitas, J. (2016). Regulação administrativa e vieses decisórios. *A&C – Revista de Direito Administrativo & Constitucional, 16*(63), 93–105.

Garcia, L. R. (2021, 29 dezembro). Boas práticas na proteção de dados: compulsoriedade ou voluntariedade? *Canal Compliance.*

Guerra, S. (2011). Função normativa das agências reguladoras: uma nova forma de atuação estatal? *Revista de Direito GV, 7*(1), 157–194.

Hahn, T. M. (2024). *Regras de boas práticas e governança em privacidade na LGPD: conceitos, controles e projeções.* Belo Horizonte: Fórum.

Heinen, L. (2017). *Autolimitação administrativa e segurança jurídica: o setor de infraestrutura brasileiro.* Tese de doutorado, Universidade Federal do Paraná.

Hogan Lovells. (2025). *The EU's Markets in Crypto-Assets MiCA regulation: A status update.* Recuperado de https://www.hoganlovells.com

Holland & Knight. (2025). *Blockchain & cryptocurrency laws and regulations 2026 – USA. Global Legal Insights.* Recuperado de https://www.globallegalinsights.com

Justen, M. (2021). *A relevância da definição de regras de boas práticas e governança pelos setores econômicos na LGPD: a necessidade de compatibilização de diversas realidades.* Curitiba: Justen, Pereira, Oliveira & Talamini.

Lacerda, C. M. V. (2021). *Regulação por princípios e julgamento profissional no setor público: um estudo sobre o regime IPSAS.* Dissertação de mestrado, Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa.

Latham & Watkins. (2025). *US crypto policy tracker – Regulatory developments.* Recuperado de https://www.lw.com

Lima, J. J. N. de. (2020). *Accountability, meta-regulação e proteção de dados pessoais na LGPD* (Tese de Doutorado, Pontifícia Universidade Católica de São Paulo).

Merkle Science. (2024). *CFTC vs. SEC: Navigating regulatory overlap in the crypto market.* Recuperado de https://www.merklescience.com

Moreira Neto, D. F. (2003). *Direito regulatório: a alternativa participativa e flexível para a administração pública de relações setoriais complexas no Estado democrático.* Rio de Janeiro: Renovar.

National Institute of Standards and Technology. (2023). *AI Risk Management Framework (AI RMF).* Recuperado de https://www.nist.gov

Pagella, J. M. (2022). *Tecnología blockchain aplicada en el registro de la propiedad.* Universidade del Salvador. Recuperado de https://racimo.usal.edu.ar

Portaldobitcoin. (2024, 22 outubro). Prefeitura de Buenos Aires lança serviço de identidade digital baseado em blockchain. Recuperado de https://portaldobitcoin.uol.com.br

Reale, M. (1994). *Lições preliminares de Direito* (27. ed.). São Paulo: Saraiva.

Rodrigues, C. H. R. (2025). Regulação responsiva e o futuro do direito regulatório. *Revista de Direito da Unigranrio, 15*(1), 121–134.

Santa Cruz. (2022). *Plan de Transformación Pública Digital – Tecnologías de registros distribuidos y blockchain.* Recuperado de https://www.saij.gob.ar

Secretaria de Governo Digital. (2020). *Guia de boas práticas – Lei Geral de Proteção de Dados (LGPD).* Brasília: Governo Federal.

Squire Patton Boggs. (2025). *MiCA legal framework: How to comply with the EU's crypto-asset rules.* Recuperado de https://www.squirepattonboggs.com

Trilateral Research. (2025, 4 setembro). *EU AI Act implementation timeline: Mapping your models to the new risk tiers.* Recuperado de https://trilateralresearch.com

U.S. Commodity Futures Trading Commission. (2025). *Digital assets – Backgrounder.* Recuperado de https://www.cftc.gov

White House. (2023). *Safe, secure, and trustworthy development and use of artificial intelligence (Executive Order).* Recuperado de https://www.federalregister.gov

White House. (2025). *America's AI Action Plan.* Recuperado de https://www.whitehouse.gov

Wired. (2025, março). The SEC is abandoning its biggest crypto lawsuits.

ZKsync. (2024, 22 outubro). *World's first ZK-backed digital identity launched in Buenos Aires.*