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

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

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

https://doi.org/10.56238/sevened2026.008-194

Sadre Pantoja Alho[1]

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.

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–

[1] Doctoral student in Legal Sciences. Universidad del Museo Social Argentino (UMSA)
E-mail: sadrepantoja@gmail.com

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.

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 INTRODUCTION

In emerging digital environments (AI and blockchain) there is tension between the need for legal certainty, that is, predictability, coherence and stability in the rules that regulate rights and responsibilities and the speed of technological innovations. While legal certainty favors decisions with *a degree of certainty* as to the legal consequences, innovation requires regulatory flexibility. As a study by the legislative branch observes, "experimentation requires predictability and legal certainty. In innovation, mistakes are expected, as long as they are not gross, because that is how... new technologies ... are developed". The challenge is to reconcile these forces, avoiding gray areas of uncertainty regarding responsibility and jurisdiction in decentralized systems without stifling innovative potential.

The central problem of this work is: how to reconcile normative predictability and the protection of rights with the speed of innovation in AI and blockchain, reducing the areas of uncertainty ("gray zones") about liability, jurisdiction, and redress in decentralized environments? This issue has great public relevance, as deregulation can undermine the confidence of users and investors, while rigid and detailed regulation can stifle technological development.

In particular, blockchain and AI-based systems generate unprecedented enforcement challenges: decentralization makes it difficult to identify who is the holder of the duty (user, developer, or platform) and which law to apply in cross-border cases. The starting hypothesis is that a hybrid regulatory model (principle + supervised self-regulation) graded by risk can offer a dynamic balance, ensuring transparency and effective means of redress even in high innovation scenarios.

The overall objective is to propose a hybrid normative model for AI and blockchain in Brazil, which combines regulation by principles (general high-level norms) with self-regulation supervised by the affected sectors, in order to differentiate duties and responsibilities according to the risk of each activity. It also seeks to establish governance mechanisms (transparency, ODR, insurance, funds) that enable effective execution of duties and reparation of damages. Specific objectives include: analyzing theories and examples of legal certainty, regulation by principles and sectoral self-regulation (e.g. art. 50 of the LGPD); (examine relevant international experiences (Europe, USA, Argentina) in blockchain and AI.

The research follows a qualitative and normative approach, combining bibliographic and documentary review. It uses analysis of constitutional principles (economic, procedural and technological) and doctrine on regulation and digital governance. A comparative study of legislation and proposals (bills and regulations) is carried out, as well as sectoral experiences (e.g., sandbox, codes of conduct). The delimitation falls on the recent Brazilian and

international context (until 2025). Key operational concepts: digital ecosystems (integrated AI and blockchain applications); regulation by principles (regulatory principles that guide, but do not standardize in detail); supervised self-regulation (standards developed by the sectors, recognized and inspected by public authority, according to LGPD art. 50); legal certainty (right to predictability and normative stability).

2 THEORETICAL-NORMATIVE FOUNDATIONS

2.1 LEGAL CERTAINTY AND REGULATION BY PRINCIPLES

Legal certainty occupies a central position in the theory of the Rule of Law and works as a minimum condition of predictability for any project to regulate digital ecosystems. At the Brazilian constitutional level, it is extracted from the set of guarantees of article 5 of the 1988 Constitution – especially the protection of acquired rights, the perfect legal act and res judicata (article 5, XXXVI) – as well as from the principles of legality, impersonality, morality, publicity and efficiency provided for in article 37, caput (Brasil, 1988). This constitutional basis indicates that the Law must ensure a minimally stable, comprehensible and predictable horizon, in order to allow individuals and organizations to plan their conduct without being surprised by sudden changes in the legal system.

Humberto Ávila develops perhaps the most influential formulation of this idea when dealing with legal certainty as a structuring principle. In his *Theory of Legal Certainty*, the author distinguishes a static dimension, linked to the knowability of Law, and a dynamic dimension, connected to the reliability and calculability of norms (Ávila, 2016). Knowability refers to the requirement that the legal system be minimally intelligible, so that the citizen can understand the content and scope of legal commands; reliability is aimed at the stability of the normative order, preventing the person from having frustrated the trust placed in a certain state of affairs; calculability, in turn, points to the need for changes to occur smoothly, allowing reasonable projections for the future (Ávila, 2016; Valiati, 2015).

To face this type of scenario, a significant portion of the doctrine points out that rigid models, entirely based on detailed rules, tend to age quickly and produce even greater informational asymmetry. Regulation by strictly casuistic commands, dependent on successive legislative changes, finds it evidently difficult to keep up with the pace of innovation (Freitas, 2016; Moreira Neto, 2005). Hence the growing attention given to the so-called regulation by principles, in which the normative core is composed of open standards – such as transparency, diligence, proportionality, equity or algorithmic accountability – which guide the actions of regulators and economic agents in new situations, not yet foreseen by

the legislator. Argumentative on the part of the regulatory agencies and the regulated themselves.

Lacerda (2021), when analyzing accounting models inspired by principles, shows that:

> The use of standards increases the space for professional judgment, but simultaneously reinforces the need for transparency of reasons and more sophisticated institutional controls. This logic can be transposed to the domain of AI and blockchain: principles such as explainability, data governance, and harm prevention do not in themselves exhaust the content of the obligation, but serve as mandatory guidance axes for regulators, developers, and platform operators.

In the current Brazilian debate, the National Petroleum Agency and the Federal Government, in documents of good regulatory practices, already recognize principle-based regulation as an appropriate instrument in sectors characterized by high innovation, precisely because it allows gradual adaptation to technological changes, without giving up minimum commands and enforcement mechanisms (National Petroleum Agency, 2019; Fonseca & Costa, 2020). Recent studies on regulatory law, in turn, describe this movement as a transition from a "command and control" model to more cooperative and responsive arrangements (Guerra, 2011; Freitas, 2016).

It is precisely at this point that the concept of responsive regulation comes in, originally developed by Ian Ayres and John Braithwaite in *Responsive Regulation: Transcending the Deregulation Debate* (Ayres & Braithwaite, 1995). The authors propose a "regulatory pyramid" in which instruments of persuasion, cooperation, and self-regulation occupy the lower rungs, while more severe sanctions and rigid commands appear at the higher levels, activated only in case of resistance or recidivism. The logic of responsiveness consists of calibrating the State's reaction according to the behavior of those regulated, combining stimuli, monitoring, and graduated punishment, with the aim of strengthening voluntary compliance and reducing supervisory costs.

In Brazil, this paradigm is beginning to be absorbed in various sectors, including the administrative law that sanctions regulatory agencies. Rodrigues (2025) describes responsive regulation as a model that seeks to reconcile normative flexibility with the preservation of the public interest, through mechanisms of listening, cooperation, and only subsequent application of sanctions, when necessary (Rodrigues, 2025).

This dialogue between legal certainty, principled regulation, and responsive regulation offers a particularly useful theoretical key for digital ecosystems. Instead of a closed set of detailed rules, what is projected is a system of structuring principles – human dignity, data protection, free enterprise, consumer protection, net neutrality, algorithmic non-

discrimination, transparency, accountability – combined with gradual enforcement mechanisms. Regulators establish mandatory, risk-based general parameters, while private actors develop codes of conduct, compliance programs, and supervised self-regulation arrangements, subject to audits, ongoing oversight, and proportionate sanctions in case of non-compliance.

In the specific field of AI and blockchain, this arrangement is compatible with the requirement of normative predictability without technological stiffening. From the point of view of legal certainty, clear and stable principles – such as the obligation to assess the impact of AI, the duty to record immutable logs in distributed networks, governance requirements, and technical documentation – allow economic agents to understand the parameters of action in advance, even if the concrete form of compliance varies according to the business model and the degree of risk. Responsive regulation, in turn, offers the tools to grade duties and reactions according to the history of compliance, the criticality of the application, and the potential for harm, preserving the ideals of knowability, reliability, and calculability highlighted by Ávila (2016).

2.2 SUPERVISED SELF-REGULATION (LGPD, ART. 50, AND SECTORAL EXPERIENCES)

Supervised self-regulation (or co-regulation) is an instrument where economic sectors develop standards of good practices that are recognized by public authority. In Brazil, the LGPD inaugurated this idea in article 50, allowing controllers and operators, alone or via associations, to formulate "rules of good practice and governance" regarding data processing

. These rules should detail organizational conditions, procedures, safety, technical standards, supervision and risk mitigation (e.g., claims from data subjects, educational actions)

. Paragraph 1 of article 50 requires that these rules consider "nature, scope, purpose, probability and severity of the risks and benefits" of the treatment, demonstrating a focus on sectoral proportionality. Once recognized by the ANPD, such rules are disclosed as a reference for the sector, constituting a kind of certificate of compliance.

In the current Brazilian debate, the National Petroleum Agency and the Federal Government, in documents of good regulatory practices, already recognize principle-based regulation as an appropriate instrument in sectors characterized by high innovation, precisely because it allows gradual adaptation to technological changes, without giving up minimum commands and enforcement mechanisms (National Petroleum Agency, 2019; Fonseca & Costa, 2020). Recent studies on regulatory law, in turn, describe this movement as a

transition from a "command and control" model to more cooperative and responsive arrangements (Guerra, 2011; Freitas, 2016).

It is precisely at this point that the concept of responsive regulation comes in, originally developed by Ian Ayres and John Braithwaite in *Responsive Regulation: Transcending the Deregulation Debate* (Ayres & Braithwaite, 1995). The authors propose a "regulatory pyramid" in which instruments of persuasion, cooperation, and self-regulation occupy the lower rungs, while more severe sanctions and rigid commands appear at the higher levels, activated only in case of resistance or recidivism. The logic of responsiveness consists of calibrating the State's reaction according to the behavior of those regulated, combining stimuli, monitoring, and graduated punishment, with the aim of strengthening voluntary compliance and reducing supervisory costs.

In Brazil, this paradigm is beginning to be absorbed in various sectors, including the administrative law that sanctions regulatory agencies. Rodrigues (2025) describes responsive regulation as a model that seeks to reconcile normative flexibility with the preservation of the public interest, through mechanisms of listening, cooperation, and only subsequent application of sanctions, when necessary (Rodrigues, 2025).

This dialogue between legal certainty, principled regulation, and responsive regulation offers a particularly useful theoretical key for digital ecosystems. Instead of a closed set of detailed rules, what is projected is a system of structuring principles – human dignity, data protection, free enterprise, consumer protection, net neutrality, algorithmic non-discrimination, transparency, accountability – combined with gradual enforcement mechanisms. Regulators establish mandatory, risk-based general parameters, while private actors develop codes of conduct, compliance programs, and supervised self-regulation arrangements, subject to audits, ongoing oversight, and proportionate sanctions in case of non-compliance.

2.3 REGULATORY LAG, HARD/SOFT LAW AND INSTITUTIONAL COORDINATION IN BRAZIL

The concept of regulatory lag refers to the mismatch between the pace of innovation and the ability to create state standards. In the digital world, products and services evolve faster than specific laws. To overcome this mismatch, *soft law instruments* (guidelines, guides, voluntary technical standards) and responsive approaches are adopted. In Brazil, there is a tendency to prioritize general norms and impact assessment when legislating innovations. The State encourages experimental regulation (e.g., financial/technological sandbox decree, cooperative self-regulation) precisely because it recognizes that "regulatory

measures without legislative approval should be preferred, given their potential for celebrated responsiveness." In other words, in the face of lag, it is preferable to delegate powers (via agencies, cooperative agreements, and administrative resolutions) than to allow sandbox or sectoral codes.

This strategy implies institutional coordination between agencies involved. For example, the ANPD has signed technical cooperation agreements with Senacon, CADE, NIC.br and TSE to align data protection with competition and open internet. The CNJ and the CNMP dialogue on judicial AI initiatives, and other regulatory agencies (SUSEP in fintechs, ANATEL in IoT) develop specific sectoral rules. However, Brazil still lacks a central integrated digital governance body. The Judiciary, in turn, deals with emerging litigation without a single standard, which reinforces the need for coherent guidelines. In this panorama, a distinction is made between hard law (laws, decrees, resolutions) and soft law (codes of conduct, recommendations, certifications). The strategic use of soft law can speed up responses without giving up regulation when necessary. Social participation and transparency (public hearings, public consultation) are crucial to legitimize this regulatory flexibility.

2.4 JURISDICTION, LIABILITY AND REDRESS IN DECENTRALIZED ENVIRONMENTS

Werbach (2018) describes blockchain as a new trust architecture, in which participants come to trust the distributed system and its consensus mechanisms, without depending on the reliability of a specific intermediary.

This form of organization, based on relative immutability, transparency, and automation of executions, reconfigures points of contact between fact and right: the "place" of the transaction no longer corresponds to a physical territory, and the very definition of who "acts" starts to involve protocol developers, infrastructure operators, token issuers, wallet providers, access platforms (front-ends), and end users. De Filippi and Wright (2018) call this environment a *rule of code*, indicating that the set of rules inscribed in the blockchain can form a kind of "lex cryptographica", still subject, however, to state orders that continue to provide sanction, legitimate coercion and reparation structures.

In terms of jurisdiction, the Law of Introduction to the Rules of Brazilian Law (LINDB) already guides the resolution of conflicts in time and space, functioning as a statute of private international law, with criteria such as the domicile of the parties, the place of the constitution of the obligation, the place where the damage occurred and the place of performance (articles 7, 9 and 12).

In decentralized environments, these elements become diffuse: the smart contract can be programmed in one country, run on globally distributed nodes, bind parties residing in

different jurisdictions, and produce economic effects in third-state markets. Finck (2019), when examining blockchain regulation and governance in Europe, underlines that decentralization tends to fragment traditional points of connection, which requires renewed focus on actors that "anchor" the network at the physical plane, such as exchanges, enterprise node operators, and user interface providers.

De Filippi and Wright (2018) highlight that many blockchain projects have attempted to present themselves as "beyond the reach" of any national authority, which has led to dramatic experiments, such as the collapse of *The DAO*, which revealed limits of purely algorithmic self-organization.

Werbach (2017; 2018) argues that:

> Blockchain and law are both trust mechanisms; Networks that ignore the incidence of state rules end up, at some point, depending on cuts, regulators, or traditional enforcement mechanisms to correct bugs, fraud, or contractual imbalances. Consequently, the difficulty does not lie in the supposed "absence of jurisdiction", but in identifying which States have sufficient connection with the litigation and on which actors decisions on liability and reparation will fall.

In the Brazilian context, the Brazilian Civil Rights Framework for the Internet (Law No. 12,965/2014) has already addressed part of these issues within the scope of centralized platforms, by disciplining the liability of connection and application providers for acts of third parties (articles 18 to 21), as well as by requiring providers operating in the country to comply with Brazilian legislation and comply with court orders. even if they are headquartered abroad (art. 11). Recent debates on the partial constitutionality of article 19, which conditioned liability to the existence of a prior court order, show that models that are excessively protective in relation to intermediaries can generate deficits in the protection of fundamental rights. The discussion still revolves around platforms such as social networks and hosting services, but the logic of gradation of responsibility as a function of control over content, economic benefit, and the ability to prevent harm offers useful parameters for environments in which smart contracts and distributed ledgers structure the provision of services.

The Brazilian experience with the responsibility of application providers in centralized platforms offers relevant lessons. Studies by Micheletti (2023) and Pereira (2022) show that the original design of article 19 of the Marco Civil worked as a containment valve for liability, by requiring a specific court order to form the duty of removal and, consequently, liability for damages arising from third-party content.

The legal evolution that has been relativizing this shielding in situations of serious violation of fundamental rights, indicates a tendency to approximate the responsibility of

digital platforms and expanded duties of care in the protection of assets such as dignity, equality and psychophysical integrity. This movement signals that, in AI and blockchain contexts, it will be difficult to accept a narrative that presents decentralization as an absolute mechanism for excluding liability, especially when there is informational and technical asymmetry to the detriment of the user.

3 INTERNATIONAL COMPARISON

3.1 EUROPEAN UNION: MICA AND AI ACT (SCHEDULE AND RISK OBLIGATIONS)

In recent years, the European Union has consolidated a regulatory bloc focused on digital ecosystems that combines the protection of fundamental rights, financial stability, and the stimulation of innovation. In the crypto field, Regulation (EU) 2023/1114, known as Markets in Crypto-Assets (MiCA), created a uniform framework for crypto-assets that were not covered by previous financial standards, with a focus on crypto-asset issuers and service providers (*CASPs*) (European Securities and Markets Authority [ESMA], 2024; European Central Bank, 2023).

MiCA structures the market into categories, such as *asset-referenced tokens* (ARTs), *e-money tokens* (EMTs), and other cryptoassets, establishing requirements for authorization, transparency, governance, and prudential rules proportional to the nature of the asset and the associated systemic risk (Hogan Lovells, 2025; Central Bank of Ireland, 2024). In issuers of stablecoins backed by currency or baskets of assets, the regulation imposes reserve requirements, liquidity management policies, disclosure rules, and volume limits, aiming to reduce run risks and financial contagion (Cyfrin, 2025; AMF, 2024).

The application schedule reinforces the gradual and risk-based logic. The text entered into force in June 2023, with the rules on ARTs and EMTs coming into force on June 30, 2024, and the rest of the regime – especially the obligations of CASPs – applicable as of December 30, 2024 (Cyfrin, 2025; ESMA, 2024).

Member states can grant a transition period of up to 18 months for already active providers, which creates a kind of "regulatory ramp" that tries to reconcile legal certainty and not sudden interruption of services (Squire Patton Boggs, 2025).

Another relevant point of MiCA is the *passporting mechanism*: once authorized in a Member State, the CASP can provide services throughout the single market, through notifications and cooperation between national authorities (Central Bank of Ireland, 2024; Hogan Lovells, 2025).

This structure reduces costs of multiple licenses, but requires intense regulatory coordination, with common supervisory guidelines and information exchange channels. In

terms of legal certainty, the main effect is to convert a mosaic of national regimes into a homogeneous set of minimum obligations, which are now valid for the entire European crypto-asset ecosystem.

In the field of artificial intelligence, the European Union approved the AI Act, described by the European institutions themselves as the first comprehensive regulatory framework aimed at AI systems. The regulation adopts a clearly risk-based approach, with a prohibition of certain practices (such as *social scoring* systems and massive real-time biometric surveillance) and a strict regime for "high-risk" systems, which need to comply with governance, documentation, risk management, data quality, and human oversight requirements (European Commission, 2025; European Parliamentary Research Service, 2025).

The implementation timeline is staggered. The bans came into effect in February 2025; as of August 2025, specific obligations for general-purpose models arise; and, in August 2026, the application of the full regime for high-risk systems begins, with an extended deadline for legacy systems until 2027 (European Parliamentary Research Service, 2025; Trilateral Research, 2025; Reuters, 2025).

The regulation also requires each member state to create at least one AI regulatory sandbox by August 2026, with the aim of testing solutions in a controlled environment and under the supervision of the competent authorities (AIAct.eu, 2025).

The literature highlights that both MiCA and the AI Act illustrate a style of regulation in which the European legislator tries to anticipate risks and establish a horizontal framework that will then be implemented by guides, technical standards, and decisions of sectoral authorities (Finck, 2019; Sartor, 2020). In terms of legal certainty, this model tends to produce greater predictability about licensing criteria, risk classification, due diligence duties, and liability possibilities, even though it creates significant regulatory costs.

Another characteristic that is of direct interest to the TCC is the connection between risk-based regulation and reparation mechanisms. In the AI Act, there is provision for robust documentation, event records, and traceability, which facilitate proof in litigation involving damage caused by AI systems (European Commission, 2025; European Parliament, 2025).

In MiCA, CASPs need to have complaint handling mechanisms, conflict of interest management policies, and procedures for handling security incidents, which opens space for integration with ODR and liability insurance (ESMA, 2024; AMF, 2024).

3.2 UNITED STATES: MULTISTEEP ARRANGEMENT OF AGENCIES (FUNCTIONAL SYNTHESIS)

The North American case follows a logic almost opposite to the European one. Instead of a single regulation for AI or cryptoassets, the country operates with a dispersed set of sectoral rules, administrative guidelines, *technical guidelines*, and multi-agency enforcement. The Congressional Research Service survey records that, until mid-2025, there was no broad federal legislation on AI, with a predominance of specific laws and administrative policies, focusing on national security, defense, privacy in specific sectors, and consumption (Congressional Research Service, 2025).

In the field of AI, the federal government has been betting on *soft law instruments*. In 2023, the National Institute of Standards and Technology (NIST) published the AI Risk Management Framework, designed as a voluntary guide for organizations that want to structure risk governance in AI, with an emphasis on reliability, transparency, fairness, and bias mitigation (NIST, 2023).

In 2023, an executive order was issued on "safe and reliable" AI development, followed by *America's AI Action Plan* of 2025, which sets public policy goals and assigns tasks to bodies such as NIST, the Department of Commerce, the Federal Trade Commission (FTC), and the Department of Justice (DOJ) (White House, 2023; White House, 2025).

The literature describes this architecture as a decentralized model, based on independent agencies, with strong use of technical guidelines and ex post enforcement. Davtyan (2025) analyzes that the North American approach is based on a combination of voluntary commitments by companies, *guidelines* from agencies such as NIST, FTC, and FDA, and repressive action by the DOJ in cases of abusive use of AI, without a single framework comparable to the AI Act (Davtyan, 2025; Associated Press, 2024).

In terms of cryptoassets, fragmentation becomes even more evident. The market is overseen by a set of bodies that includes the Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission (CFTC), the Department of the Treasury (via FinCEN and OFAC), federal banking regulators (Federal Reserve, OCC, FDIC), as well as state agencies responsible for securities transfer licenses and consumer protection (Latham & Watkins, 2025; Holland & Knight, 2025).

The SEC generally classifies certain cryptoassets as securities, based on the *investment contract test* derived from *SEC v. Howey Co.*, and oversees public offerings, exchanges, and *tokens* that qualify as securities (Merkle Science, 2024; SEC, 2025).

The CFTC treats cryptoassets as commodities in derivatives markets, with jurisdiction over futures contracts, *swaps,* and margin markets, in addition to overseeing manipulation and fraud (CFTC, 2025; WilmerHale, 2025).

A recent report on the blockchain and crypto regulatory framework in the U.S. describes this arrangement as dynamic overlap: SEC and CFTC vie for spaces of competence, while FinCEN applies anti-money laundering standards and OFAC controls sanctions, generating a scenario in which the same platform may be subject to multiple chains of obligations, often with interpretive divergences (Holland & Knight, 2025).

In the field of liability, the absence of a single framework means that traditional principles of *securities law*, consumer protection, and civil liability are projected on cases involving AI and cryptoassets. The FTC has been signaling that deceptive practices associated with AI – for example, unsubstantiated claims about system capabilities – can be framed as *unfair or deceptive acts or practices*, while the DOJ has already announced that the use of AI to intensify white-collar crimes can aggravate penalties (Department of Justice, 2024).

At the federal level, state initiatives to regulate AI and crypto are increasing, which has led to discussions about an eventual executive order to limit state laws considered overly restrictive (Politico, 2025).

From the perspective of legal certainty, this multi-steep arrangement produces important ambiguity. There is a high capacity for reaction on the part of agencies, which can issue quick guidelines and act in enforcement, but economic agents deal with uncertainty about the legal classification of assets, the boundary between the competence of the SEC and the CFTC, the incidence of state rules and the possibility of changes in guidance according to the Administration in office (Wired, 2025; Latham & Watkins, 2025). At the same time, this model reveals useful instruments for interagency coordination and intensive use of technical standards and *guidelines* that can inspire responsive arrangements in the Brazilian context.

3.3 ARGENTINA: REGISTRY DIGITIZATION, DIGITAL IDENTITY/SIGNATURE, AND AI/BLOCKCHAIN INITIATIVES

The Argentine experience offers an example of a Latin American country that consolidated, relatively early, a legal basis for digital documents and signatures and has progressively been incorporating distributed ledger technologies into digital government policies and sectoral initiatives. Law No. 25,506 of 2001 instituted the digital and electronic signature regime, recognizing the legal effectiveness of digitally signed electronic documents

and creating the Digital Signature Infrastructure of the Argentine Republic (IFDRA) (Argentina, 2001; Argentina.gob.ar, 2016).

Subsequent norms, such as Law 27,446 and regulatory decrees, updated this framework, integrating the digital signature into the electronic document management of the Public Administration and encouraging its use in contracts, administrative petitions, and registration acts (Argentina.gob.ar, 2016; Ecertla, 2023).

The doctrine points out that this arrangement conferred on the digital signature a status equivalent to that of the handwritten signature, provided that certification and integrity requirements were respected, which allowed the expansion of digital legal services, such as electronic orders and distance notarial procedures (CheersContracts, 2025).

In the field of registry digitization, several projects explore the use of blockchain as an additional layer of reliability. A study by Pagella (2022) analyzes the application of blockchain in the Real Estate Property Registry of the Federal Capital, evaluating potential gains in authenticity, immutability, and traceability of registration acts (Pagella, 2022).

The same line appears in projects such as the Public Registry of University Graduates, whose database, linked to the Ministry of Education, has started to use blockchain to authenticate diplomas and academic transcripts, allowing third parties to verify the veracity of the information in a public and auditable way (Blockchain Federal Argentina, n.d.).

There are also regional normative initiatives that explicitly mention distributed ledgers. The Digital Public Transformation Plan of the province of Santa Cruz, for example, authorizes the Executive to employ distributed ledger technologies and blockchain networks, public or private, in digital government services, teleworking, and administrative processes, with a view to increasing transparency and trust (Santa Cruz, 2022).Saij Public petitions submitted to national authorities request the incorporation of blockchain into public registries on the grounds that the technology could reduce corruption, fraud, and delays in registration procedures (Change.org, 2025).

The most visible case in the international debate, however, is the decentralized digital identity project of the city of Buenos Aires. In 2024, the capital launched the QuarkID system, integrated with the miBA application, with the proposal to offer blockchain-based digital credentials, supported by zero-knowledge proofs, which allow citizens to demonstrate attributes (such as age or educational status) with minimal exposure of personal data (Borak, 2024; Coindesk, 2024; ZKsync, 2024).

Official reports indicate that the project aims to reach around 3.6 million residents, configuring the first decentralized identity initiative enabled by a municipal government on a scale of this magnitude (Dig.watch, 2024; ZKsync, 2024).

The logic behind QuarkID is associated with the idea of *self-sovereign identity (SSI),* in which the holder maintains control over his credentials, which can be verified by third parties without the need to retain data in large centralized databases. From the point of view of legal certainty, this experience shows an effort to reconcile fundamental privacy rights, robust authentication, and record integrity requirements. The choice of protocols with zero-knowledge proofs indicates an explicit concern with proportionality in data exposure and with the possibility of technical auditing of validation mechanisms (Portaldobitcoin, 2024; Chainwire, 2024; BrazilCrypto, 2024).

It is also possible to observe that the advancement of registry digitization and digital identity projects in Argentina occurs in dialogue with the digital signature framework and the existing certification infrastructure. The dominant interpretation maintains the idea that electronic documents signed with a valid certificate enjoy a presumption of authenticity and integrity, which facilitates the integration between traditional records and solutions based on blockchain and AI, used as additional layers of proof or automation of verifications (Argentina.gob.ar, 2016; CheersContracts, 2025).

Together, these elements make up a scenario in which Argentina combines, on the one hand, a relatively consolidated legal basis in terms of documents and digital signatures; on the other, experimental pilots in decentralized identity and the use of blockchain in public records, still in the maturation phase, but relevant as a normative laboratory for the region.

3.4 COMPARATIVE SYNTHESIS AND LESSONS FOR BRAZIL

The comparison between the European Union, the United States, and Argentina reveals three distinct ways of facing the legal risks associated with AI, cryptoassets, and distributed ledgers. The European model, represented by MiCA and the AI Act, favors horizontal and detailed regulations, anchored in a risk approach and combined with clear timelines, regulatory sandboxes, and structured supervisory mechanisms. The main consequence is a high degree of predictability regarding risk categories, authorization requirements and possible sanctions, with high regulatory costs and strong centrality of European authorities.

The North American arrangement, in turn, is supported by a network of agencies with competences over fragments of the digital ecosystem. The absence of an AI Act or a federal MiCA means that *securities law*, consumer law, anti-money laundering, competition, and data protection standards are projected on AI and blockchain on a case-by-case basis, complemented by technical *guidelines* such as the NIST AI RMF and executive orders (NIST, 2023; Davtyan, 2025; Congressional Research Service, 2025).

This reinforces flexibility, but increases uncertainty regarding the future of interpretations and the division of competence between agencies such as the SEC, CFTC, FTC, FinCEN, and state regulators (Latham & Watkins, 2025; Holland & Knight, 2025).

The Argentine experience occupies an intermediate position. The country has consolidated, with Law 25.506 and updates, a relatively cohesive digital signature and electronic document regime, which serves as a basis for digitizing services, administrative processes and records. From this base, projects for the use of blockchain in property records and diplomas emerge, as well as the QuarkID initiative in Buenos Aires, with decentralized digital identity supported by zero-knowledge proofs (Pagella, 2022; Blockchain Federal Argentina, n.d.; Dig.watch, 2024; ZKsync, 2024).

For the Brazilian debate on legal certainty in digital ecosystems, these three experiences generate some central lessons, directly related to the hypothesis of a hybrid model based on regulation by principles and supervised self-regulation:

Grading duties by risk, as in the AI Act and MiCA, is compatible with the idea of modulating obligations along the protocol, infrastructure, enforcement, and intermediation layers, including in the context of public registries and AI applied to notarial and registry services.
Passportization and mutual recognition of compliance programs, typical of MiCA, point the way for codes of conduct and governance programs in AI and blockchain in Brazil to be recognized by sectoral authorities, with effects on different markets, reducing the costs of multiple authorizations.
Interagency coordination, although unequal in the North American model, provides examples of mechanisms for articulation between financial agencies, consumer protection, data protection, and competition, a relevant aspect in view of the overlap between the Central Bank, CVM, Cade, ANPD, and the Judiciary on the topic of AI/blockchain.
Anchoring in digital identity and signature frameworks, as observed in Argentina, indicates that any blockchain-based registry ecosystem design needs to dialogue with the existing infrastructure of ICP-Brasil, digital certification, advanced signatures, and new identification models, including decentralized solutions compatible with data protection rights (ZKsync, 2024).

From this perspective, the international comparison reinforces the plausibility of the SIM (Sustainability–Interoperability–Regulatory Framework) hypothesis applied to Brazilian public registries.

The institutional sustainability of services, technical-normative interoperability and the construction of a regulatory framework that combines clear principles, supervised self-regulation and effective instruments of execution and reparation are found in the European, North American and Argentine experience.

4 CONCLUSION

In summary, the article started from the observation that the expansion of digital ecosystems based on artificial intelligence and blockchain intensifies a classic dilemma of the Rule of Law: on the one hand, the requirement of legal certainty, translated into predictability, minimum stability, and the possibility of calculating the legal consequences of conduct; on the other hand, the need for sufficient normative openness so as not to stifle innovation processes that develop in cycles much faster than legislative time. The initial question — how to reconcile normative predictability and protection of rights with the speed of innovation in decentralized environments — guided the analysis of constitutional foundations, regulatory models, and foreign experiences, allowing us to propose an intermediate path between deregulation and excessive legal detail.

The reconstruction of legal certainty as a structuring principle showed that it is not reduced to the literal conservation of norms, but involves knowability, reliability and the possibility of planning. From there, the work indicated that a model strictly based on rigid, casuistic, and frequently changed rules tends to aggravate uncertainty in complex technological contexts, as it generates successive "layers" of regulation that are unable to keep up with reality. On the other hand, regulation by principles and responsive regulation emerge as more appropriate alternatives for digital ecosystems: principles such as transparency, prevention, proportionality, and data governance work as stable normative axes, while responsiveness allows calibrating state action according to the risk of the activity and the behavior of the agents.

Within this framework, supervised self-regulation gained special prominence. Recent experience in data protection, with codes of conduct and governance programs recognized by specialized authorities, shows that economic sectors and public agencies can take responsibility for the implementation of standards, as long as they remain subject to constitutional and legal parameters. Instead of a State that tries to anticipate, alone, all technical solutions, a dynamic is designed in which regulators define objectives, principles, and risk benchmarks, while regulated subjects detail operational standards in dialogue with these benchmarks, under monitoring, auditing, and the real possibility of sanction. Such an arrangement demonstrates potential to deal with rapidly changing technologies, without giving up public control or channels of accountability and reparation.

The analysis of jurisdiction, liability, and redress in decentralized environments has shown that the "lawlessness" narrative in blockchain and distributed AI does not hold water. Decentralization complicates the mapping of who acts, where they act, and with which law they are bound, but it does not eliminate the presence of identifiable actors who design

protocols, maintain infrastructures, operate interfaces, and economically exploit digital services. The conclusion that is required is that legal certainty in these ecosystems depends on the construction of a network of graduated responsibilities, distributed across the layers of protocol, infrastructure, application, intermediation and use, with more intense duties for those who have greater technical and economic capacity to prevent damages, without completely excluding the co-responsibility of users when they act intentionally or in manifest contravention of the established rules.

The comparative examination of the European Union, the United States and Argentina reinforced this perception. The European model, with comprehensive regulations and a risk-based approach, shows that it is possible to establish clear categories, implementation schedules and mandatory sandboxes, generating a high degree of predictability, even at the cost of greater regulatory density. The North American arrangement, more fragmented and based on multiple agencies and soft law instruments, reveals a great capacity for reaction and adaptation, but also significant uncertainty regarding the distribution of competences and the future of interpretations. The Argentine experience, by consolidating a regime of documents and digital signatures and from it experimenting with blockchain applications in records and digital identity, highlights the importance of a well-defined legal basis for innovative projects to find institutional and evidentiary anchorage.

When this set of elements is projected on the universe of Brazilian public records, the hypothesis of a hybrid model based on the triad Sustainability-Interoperability-Regulatory Framework gains consistency. Sustainability refers to the economic and institutional viability of services in the face of intensive digitalization, including investments in technological infrastructure, information security, and team training. Interoperability involves building technical and regulatory solutions that allow distributed ledgers, metadata, APIs, and AI systems to converse with registry legislation, civil procedure, public key infrastructure, and personal data protection, in order to ensure evidentiary admissibility, traceability, and auditability. The regulatory framework component, on the other hand, refers to the need to explain, in general rules and supervised self-regulation instruments, who is responsible for which risks in each layer of the digital registry ecosystem, with concrete instruments of protection, such as ODR, insurance, and compensation funds.

From this path stems a central conclusion: legal certainty in digital ecosystems does not require the paralysis of innovation, but rather the construction of an environment in which relevant innovations are developed within a minimally stable framework of principles, duties and consequences. A hybrid model, based on regulation by principles, responsive regulation, and supervised self-regulation, with grading of duties by risk and sectoral application to public

registries under the SIM hypothesis, is capable of reducing gray areas of liability, jurisdiction, and redress in decentralized environments, without stifling technological experimentation. The need to deepen the practical application of these guidelines in pilot projects, to empirically measure their effects in terms of efficiency, trust and reduction of litigation, and to adjust, based on these results, the proposed governance matrix remains open. The point of arrival of this article, therefore, is the assertion that the challenge posed by AI and blockchain to Brazilian Law is not merely technological, but institutional and hermeneutic, and that its most promising response lies in a balanced combination of clear principles, regulatory cooperation, and shared responsibility.

REFERENCES

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). 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. 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. https://servicios.infoleg.gob.ar

Argentina.gob.ar. (2016). Normativa de firma digital. 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. https://bfa.ar

Borak, M. (2024, 23 outubro). Buenos Aires moves from centralized to decentralized digital identity with QuarkID. Biometric Update. 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. https://newsletter.brazilcrypto.io

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

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

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

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

Congressional Research Service. (2025). Regulating artificial intelligence: U.S. and international approaches (R48555). 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. 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). https://scholarlycommons.law.case.edu

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

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

European Parliamentary Research Service. (2025). AI Act implementation timeline (PE 772.906). 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. https://www.hoganlovells.com

Holland & Knight. (2025). Blockchain & cryptocurrency laws and regulations 2026 – USA. Global Legal Insights. 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. 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. 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). https://www.nist.gov

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

Portaldobitcoin. (2024, 22 outubro). Prefeitura de Buenos Aires lança serviço de identidade digital baseado em blockchain. 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. 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. https://www.squirepattonboggs.com

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

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

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

White House. (2025). America's AI Action Plan. 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.