A Necessary Cognitive Turn in Digital Constitutionalism: Regulated Self-Regulation as a Regulatory Mechanism for Artificial Intelligence (AI) in Comparative Law

Ricardo Campos

Abstract: This paper argues that the debate on digital constitutionalism suffers from a deficit in the cognitive dimension of knowledge generation, focusing predominantly on normative principles and values while neglecting the significant challenge of law's capacity to generate knowledge for its own application. To address this gap, the paper examines regulated self-regulation as an effective mechanism for regulating artificial intelligence (AI) in both European and Brazilian legal contexts. The introduction outlines the growing impact of AI on citizens' rights and emphasizes the need for regulatory frameworks that balance innovation with public interest protections. The first section critiques the theoretical and practical limitations of digital constitutionalism in managing the challenges posed by AI. The subsequent section analyses how regulated self-regulation can bridge the divide between state regulation and self-regulation, using the European General Data Protection Regulation (GDPR) and Brazil's General Data Protection Law (LGPD) as case studies. In conclusion, the paper underscores the potential of regulated self-regulation to promote ethical AI development, safeguard fundamental rights, and foster innovation through adaptive governance and stakeholder collaboration, particularly by enhancing the generation of legal knowledge required for effective law enforcement.

A. Introduction

Artificial intelligence is increasingly becoming part of our daily lives. As the technology advances and gains more popularity, concerns are being raised about its impact on citizens' rights, encompassing ethical, legal, and socioeconomic questions. In recent years, efforts have been made to strike a proper balance between technological innovation and the protection of public interests and individual rights, which is reflected in a variety of regulatory approaches.

It is extremely challenging to reach a consensus that addresses the different legal perspectives associated with adopting universally applicable AI regulations. Nonetheless, certain regulatory initiatives, such as UNESCO's[1] and OECD's[2] recommendations for the development and use of technology, seem to be moving in this direction: although there are differences in content and in the form of implementation of the guidelines, respect for privacy and the protection of personal data, the need for accountability systems, and the requirements of security, transparency, explainability, and non-discrimination appear to form a common thread across various regulatory instruments[3].

The issue, however, is that these documents, while symbolizing an universal goodwill towards regulating AI, contain general and voluntary principles and obligations, which rightfully face criticism for neglecting the economic and political interests driving the current gold rush. As a result, many nation-states are also attempting to organize their own internal structures and norms according to their specific social, economic, and political characteristics, either by establishing "mere" ethical principles to guide AI development or by setting more robust and stringent rules.

The European Union, for example, has sought to develop a regulatory approach that fosters the introduction of AI while addressing its associated risks. This involves a legal framework aimed at creating an ecosystem of trust between companies and consumers while also accelerating the adoption of technology in Europe. To this end, the EU faced the challenge of defining AI in a way that is flexible enough to accommodate the technology's dynamic nature, while effectively applying a risk-based approach that considers its advantages without over-regulating it. The proposed regulation on AI – known as "AI Act" – was published in 2021[4].

---

1 Unesco, *Recommendation on the Ethics of Artificial Intelligence*, Adopted at the 41st session of the UNESCO General Conference, November 23, 2021. Accessed on October 23, 2024. https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence.

2 OECD, *Recommendation of the Council on Artificial Intelligence*, Adopted by the OECD Council on May 22, 2019. Accessed on October 23, 2024. https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449.

3 See, in general, Floridi, L., *The ethics of artificial intelligence: principles, challenges, and opportunities*. New York, 2023, p. 57 ff.

4 This has led to various criticisms of regulation in a scenario of uncertainty amidst a new industrial revolution. For the negative impacts on the European economy, see Mario Draghi, *The Future of European Competitiveness*, 09.2024.

Unlike in the EU, regulations in the United States are generally developed in a decentralized and vertical manner at the level of individual states and sectors[5].The former US President, Joe Biden, intended to change this trend by issuing an order titled "Executive Order on the Safe and Trustworthy Development and Use of Artificial Intelligence"[6], which establishes a series of voluntary commitments that must be fulfilled by companies wishing to develop and deploy this technology in the country. However, the Executive Order has been recently revoked by Donald Trump[7].

Another example that must not be overlooked is China's[8], the country with the most stringent regulations in this area, with specific laws on issues such as algorithmic recommendations and deep manipulation of content. In contrast to the European and (the previous) American approaches, the Chinese strategy involves strong state intervention as a differentiating factor[9], which firstly promotes the strengthening of the domestic market and secondly leads to a hegemonic position in the global development of tech-

5 Williams, A. *What Could Horizontal AI Legislation Look Like In the US? Exploring the US Algorithmic Accountability Act*. In: HolisticAI Blog, January 9, 2023. Available online at: https://www.holisticai.com/blog/us-algorithmic-accountability-act, last accessed: May 7, 2024. For a comparative perspective between the American and European approaches, see: Mökander, J. et al. *The US Algorithmic Accountability Act of 2022 vs. The EU Artificial Intelligence Act: What Can They Learn from Each Other?* In: Minds and Machines, Vol. 32, No. 4, pp. 751–758, December 1, 2022.

6 U.S. White House. *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*. October 30, 2023. Available online at: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/, last accessed: October 9, 2024.

7 Reuters, "Trump revokes Biden executive order addressing AI risks," 2025. Accessed on February 6, 2025: https://www.reuters.com/technology/artificial-intelligence/trump-revokes-biden-executive-order-addressing-ai-risks-2025-01-21/.

8 For a general overview of China's regulatory context, see: Roberts, Huw et al. *The Chinese Approach to Artificial Intelligence: An Analysis of Policy, Ethics, and Regulation*. In: *Ethics, Governance, and Policies in Artificial Intelligence*. Philosophical Studies Series, Vol. 144, Springer, 2021, pp. 47–79. Available online at: https://link.springer.com/chapter/10.1007/978-3-030-81907-1_5, last accessed on: October 9, 2024.

9 For comparative approaches between China's regulatory context and the respective American and European contexts, see: Hine, Emmie; Floridi, Luciano. *Artificial Intelligence with American Values and Chinese Characteristics: A Comparative Analysis of American and Chinese Governmental AI Policies*. In: *AI & Society*, Vol. 39, pp. 257–278, 2024. Available online at: https://link.springer.com/article/10.1007/s00146-022-01499-8, last accessed on: October 9, 2024; and Dixon, Ren Bin Lee. *Artificial Intelligence Governance: A Comparative Analysis of China, the European Union, and the United States*. Master's thesis, May 2022.

nology. The Chinese strategy involves a close alignment between the state and the country's leading AI companies, which brings us to an interesting point in the discussion about regulating this technology. According to a report by the Washington Post, during their first meeting with companies regarding algorithm regulation, state representatives showed "little understanding of the technical details," which prompted company representatives to use a combination of metaphors and simplified language to address the topic. This highlights that, from an innovation perspective, relying solely on the state apparatus to establish standards and development guidelines for AI (and other emerging technologies) can have negative consequences.

In this regard, it should be noted that in the current context of the increasing *algorithmization* of human life, the law, as a fundamental part of the normative structure of society, is now facing pressures it had not encountered until relatively recently. The recent introduction of legal regulations for the protection of personal data worldwide is an excellent example that clearly illustrates how one of the functions of modern law is to align normative (legal) levels with new technologies.[10]

This is because technological revolutions are always intertwined with the current intellectual, social, political, and economic context, deeply integrated into these aspects, and have collateral effects. Technological revolutions lead to the deconstruction of previously established concepts, paradigms, structures, and identities, contributing to their critical reassessment in light of the new stage of technological and societal development.[11] The sociologist Niklas Luhmann had already expressed theoretical doubts in the 1990s about the future development of law in a society shaped by an emerging technological revolution[12]. His works reflect a search for understanding a society that increasingly focuses on new technologies and their cross-border impacts, for which the traditional mechanisms of law and

10 V. Descombes, *Die Rätsel der Identität*, Berlin 2013, pp. 226 ff; T. Vesting, *Gentleman, Manager, Homo Digitalis. Der Wandel der Rechtssubjektivität in der Moderne*, Weilerswist 2021.

11 M. Beloy, *Post-humaner Konstitutionalismus? Eine kritische Verteidigung der anthropozentrischen und humanistischen Traditionen in der algorithmischen Gesellschaft*, in: M. Beloy (ed.), *The IT Revolution and its Impact on State, Constitutionalism and Public Law*, Oxford 2021.

12 In this regard, see, among other works, Luhmann, N, *Die Politik der Gesellschaft*, Frankfurt am Main, 2002, p. 220.

politics, centred around the nation-state, can no longer play the same role as before[13].

The connection between law and the protection of the individual (and their fundamental rights and prerogatives) therefore seems to be a more complex challenge than it was when the structuring of social norms was centred on the state as a regulator. Particularly with the emergence of new computer, information, and communication technologies, the normative structures that shape the exercise of rights can no longer be influenced or enabled solely by state actions. It is no exaggeration to say that "a state-centred view of lawmaking has become unrealistic and insufficient"[14]. This is especially true since digitalization has led to an increase in the asymmetry of knowledge between the regulatory state and private society. Increasingly, knowledge resides in private society and the great challenge for the state becomes how to create institutionalized procedures to generate knowledge for the application of the law.

In this way, new normative constructions tend to structure the scope of action for individuals, companies, and the State based on the modelling of the environment itself and the design of the business model that underlies the development of these new technologies. This, incidentally, represents the modern character of law: it deals with an indefinite and indeterminable complexity of factors, but is also a driving force for the construction of new and complex social relationships[15].

Although a number of scholars and legal practitioners have turned to the so-called "digital constitutionalism" as a legal theory capable of addressing the issues arising from the digitalization of society, I will argue in this paper that the concept is somewhat insufficient. This is because new forms of knowledge production in the digital society require actions that go beyond traditional state intervention, while also avoiding exclusive reliance on the self-regulation proposed by private actors. In this regard, I will seek to analyse how regulated self-regulation emerges as a suitable approach to guide the creation (or adaptation) of rights in response to the challenges of the digital era.

13 Luhmann, N., *Die Wirtschaft der Gesellschaft*, Frankfurt am Main, 1994, p. 170 ff.; Luhmann, N., *Die Gesellschaft der Gesellschaft*, Frankfurt am Main, 1997, p. 166 ff.

14 T. M. Hahn, *Código de conduta. Autorregulação na Lei Geral de Proteção de Dados Pessoais: conceitos, controles e projeções*, 2024, in press, p. 15.

15 R. Campos, *Metamorfoses do Direito Global: Sobre a Interação Entre Direito, Tempo e Tecnologia*, São Paulo, 2022.

B. Theoretical and practical shortcomings of digital constitutionalism

The recent reflections on what has been called *digital constitutionalism* emerge within a political, social, and economic context heavily shaped by the concept of the "Platform Society"[16]. In light of the inefficacy in applying existing regulatory frameworks and the absence of specific legal provisions for innovative practices, digital platforms have branched out without being fully subjected to the legal and social responsibilities regarding how these environments are structured and how the exercise of power within them can be limited[17]. Within this landscape, digital constitutionalism is broadly viewed as a concept employed by theories that seek to provide interpretative frameworks for public, private, and hybrid actions, with the goal of mitigating the concentration of economic and political power by these actors.

The disruptive impact of digital technologies is acting as a catalyst for a "new constitutional moment"[18] by challenging existing legal, political, and social norms. In response, societies must adapt their constitutional frameworks to accommodate the changes brought about by the digital age, resulting in potential shifts in fundamental rights and governance structures. These changes lead to an alteration of what is commonly called "constitutional balance," which would be an ideal condition produced by the application of constitutional law norms in a given legal order[19]. In other words, by affecting the protection of fundamental rights and the balance of powers, new technologies (especially digital platforms) would have promoted a disturbance of this balance, which in turn would have triggered the so-called "normative counteractions" as a response, with the purpose of restoring the previous state[20].

16 J. van Dijck, D. Nieborg, T. Poell, *Reframing platform power*, in: Internet Policy Review, Vol. 8, No. 2, 2019, pp. 1-18, p. 2.

17 N. P. Suzor, Digital Constitutionalism: Using the Rule of Law to Evaluate the Legitimacy of Governance by Platforms, in: Social Media + Society, Vol. 4, No. 3, 2018, pp. 1-11, p. 2.

18 "Contemporary society is experiencing a new constitutional moment, whose main catalyst is the disruptive impact of digital technology". E. Celeste. Digital Constitutionalism: a new systematic theorization. Internet Review of Law, Computers & Technology, v. 33, n. 1, p. 77.

19 Celeste, Edoardo. Digital Constitutionalism: a new systematic theorization, fn. 18.

20 Celeste, Edoardo. Terms of service and bills of rights: new mechanisms of constitutionalisation in the social media environment? Internet Review of Law, Computers & Technology, v. 33, n. 2, p. 133.

These counter-actions would consist in initiatives of integration or amendments to the existing normative framework[21], and could arguably be guided by *digital constitutionalism*, a concept that represents a set of values and principles that permeate, inform and guide the process of constitutionalization of the digital environment[22]. For digital constitutionalism, the reactions to the disturbances that new technologies have brought to the "constitutional balance" should be based on already existing constitutional principles, in a polycentric process – which has been commonly called "constitutionalization" – that may involve different instruments, either within the dimension of the States (such as legislations and decisions of constitutional courts) or outside the States (example of Internet charters of rights, even if they are not binding) [23].

For certain scholars, digital constitutionalism may manifest through advanced regulatory models. Giovanni de Gregorio, for instance, in discussing recent regulatory initiatives, identifies this manifestation within the European Union, specifically referring to the European Digital Services Act as a "reaction to new digital powers" following a period in which, in his view, the regulation of the bloc had neglected and overlooked the role of constitutionalism and constitutional law in safeguarding fundamental rights and in limiting the growth and consolidation of unaccountable powers that abuse constitutional values.[24] Another expression of digital constitutionalism — highlighting the flexibility of the concept[25] — is its connection to institutional initiatives in the realm of self-regulation. A possible example, framed within the theoretical structure provided by digital

21 "[T]hese counteractions consist in the integration or in the amendment of the existing normative framework and aim to restore a condition of relative equilibrium in the constitutional system". Celeste, Edoardo. Digital Constitutionalism: a new systematic theorization, fn. 10.

22 "[It] represents the set of values and ideals that permeate, inform and guide the process of constitutionalisation of the digital environment". Celeste, E. Digital Constitutionalism: a new systematic theorization. Internet Review of Law, Computers & Technology, v. 33, n. 1, p. 90.

23 E. Celeste, What is digital constitutionalism?, in: The Digital Constitutionalist, available at: https://digi-con.org/what-is-digital-constitutionalism/.

24 G. de Gregorio, Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society, Cambridge 2022, p. 3.

25 J. R. G. Pereira, C. I. Keller, Constitucionalismo Digital: contradições de um conceito impreciso, in: Revista Direito e Práxis, Vol. 13, No. 4, Dezember 2022, pp. 2648–2689, p. 2674, available at: https://doi.org/10.1590/2179-8966/2022/70887.

constitutionalism[26], is the Facebook Oversight Board, created by Meta in 2019 to serve as a secondary instance for reviewing content moderation decisions made on the platform.

Specifically in the Brazilian context, Saavedra and Borges argue that Brazil currently experiences a phase of digital constitutionalism[27]. This inclination toward the ideology is evidenced, first and foremost, by the broad debates surrounding internet legislation, most notably the Marco Civil da Internet (MCI), which saw significant public participation—an unprecedented occurrence at the time. There is also a growing concern for established constitutional rights, such as privacy and intimacy. Moreover, fundamental principles such as net neutrality and informational self-determination would be likewise protected, reflecting a clear trend in the country toward digital constitutionalism. In further examining the Brazilian scenario, Mendes and Ferreira suggest that, within state structures, "the principles and values of digital constitutionalism can serve as normative standards for the judicial review of internet-related legislation"[28]. According to the authors, digital constitutionalism would influence, through judicialization, the redefinition of "the essence of fundamental constitutional rights related to freedom of expression, protection of honour, and privacy" in the face of the current technological landscape[29].

Regarding the concept itself[30], Suzor conceives digital constitutionalism as a project aimed at articulating and establishing standards and legitimacy for governance in the digital age, which involves assessing the internal governance mechanisms of private platforms in light of "the principles

26 M. Miloš, T. Pelić, Constitutional Reasoning There and Back Again: The Facebook Oversight Board as a Source of Transnational Constitutional Advice, in: J. de Poorter et al. (Ed.), European Yearbook of Constitutional Law 2021: Constitutional Advice, Vol. 3, The Hague 2022, pp. 197-223.

27 G. A. Saavedra, G. O. A. Borges, Constitucionalismo Digital Brasileiro, in: Revista da AJURIS, Vol. 49, No. 152, Oktober 2022, pp. 157–180, available at: http://revistadaajuris.ajuris.org.br/index.php/REVAJURIS/article/view/1228.

28 G. Ferreira Mendes, V. Oliveira Fernandes, Constitucionalismo Digital e Jurisdição Constitucional: uma agenda de pesquisa para o caso brasileiro, in: Revista Justiça Do Direito, Vol. 34, No. 2, 2020, pp. 6-51, p. 3, available at: https://doi.org/10.5335/rjd.v34i2.11038.

29 G. Ferreira Mendes, V. Oliveira Fernandes, Constitucionalismo Digital e Jurisdição Constitucional, fn. 28.

30 Para uma visão geral sobre como diferentes autores abordam o conceito de constitucinalismo digital, cf. E. Celeste, Digital Constitutionalism: A New Systematic Theorisation, in: International Review of Law, Computers & Technology, Vol. 33, No. 1, Januar 2019, pp. 76–99, available at: https://doi.org/10.1080/13600869.2019.1562604.

of the Rule of Law" [31]. Celeste, in turn, views digital constitutionalism as a variation of modern constitutionalism, which demands the creation of normative countermeasures to address the shifts in constitutional balance brought about by the advent of digital technology, while also providing the ideals, values, and principles that guide such countermeasures[32]. In this sense, digital constitutionalism represents a "set of values and principles that influence, guide, and underpin the process of constitutionalizing the digital environment"[33]. Alternatively, the concept can be seen as "a useful shorthand to denote the theoretical strand that advocates for the translation of the core values of constitutionalism in the context of the digital society"[34].

Pereira and Keller identify two categories of issues related to the limitations and possibilities of the concept of digital constitutionalism. The first concerns the explanatory value and normative appropriateness of expanding the concept of a constitution to include legal forms that, in many respects, differ from those that shaped constitutionalism as established by modern political theory; the second relates to the risks and implications associated with broadening the concept of constitutionalism, as well as the recent uses of the category of digital constitutionalism[35]. A similar critique can be found in Trindade and Antonelo, who argue that the concept of digital constitutionalism—in a broad and superficial sense—serves merely as a "crutch" for the process of constitutionalizing the digital environment[36]. According to these authors, the concept is a dispensable support, like an accessory, as it adds nothing new, conceptually or substantively, to the idea of constitutionalism, particularly contemporary constitutionalism, and thus

31 N. P. Suzor, Digital Constitutionalism: Using the Rule of Law to Evaluate the Legitimacy of Governance by Platforms (Fn. 9), p. 2.

32 E. Celeste, Constitucionalismo digital: mapeando a resposta constitucional aos desafios da tecnologia digital, in: Revista Brasileira de Direitos Fundamentais & Justiça, Vol. 15, No. 45, 2021, pp. 63–91, p. 81.

33 E. Celeste, Constitucionalismo digital: mapeando a resposta constitucional aos desafios da tecnologia digital, fn. 33.

34 E. Celeste, Constitutionalism in the Digital Age, in: J. Pohle et al. (Ed..), Liber Amicorum for Ingolf Pernice, HIIG Book Series, 2020.

35 R. G. Pereira, C. I. Keller, Constitucionalismo Digital: contradições de um conceito impreciso (Fn. 24), p. 2676.

36 A. Trindade, A. Antonelo, Constitucionalismo digital: um convidado (in)esperado, in: Revista Brasileira de Direito, Vol. 18, No. 1, 2023, p. 13, available at: https://doi.org/10.18256/2238-0604.2022.v18i1.4816.

cannot justify the creation of a specific or segmented form of constitutionalism[37].

Even if one were to accept the concept of digital constitutionalism as a normative model or legal theory, or to endorse a possible "reconciliation" of the various conceptualizations of the ideology in question[38], at least one more critique can be raised regarding the use of digital constitutionalism as a theory capable of solving the problems arising from digitalization. In summary, digital constitutionalism seeks to expand the normative structure of traditional constitutionalism by aligning its values and principles with the rapidly changing digital environment of modern society. However, this approach exposes an inherent limitation, particularly in confronting a defining aspect of the digital era: the increasing prevalence of the cognitive dimension over the normative one[39]. Amidst this ongoing transformation, the legal framework itself is undergoing substantial changes, rendering it insufficient to rely solely on the values and principles of conventional constitutionalism. In other words, it is necessary to go beyond merely appealing to principles, aiming to reconcile the new forms of knowledge generation in the platform society with effective and efficient ways of translating these principles into practical applications[40]. As will be discussed in the following sections of this paper, one possible solution is the establishment of regulated self-regulation within the context of new digital technologies.

C. Self-Regulation Based on Experiences with the Protection of Personal Data

I. Regulated self-regulation as a mean of knowledge generation

One of the most efficient ways to enhance the new ways of knowledge generation is through regulated self-regulation. Self-regulation, which emerged

37 A. Trindade, A. Antonelo, Constitucionalismo digital: um convidado (in)esperado,fn. 36.

38 E. Celeste. "Digital Constitutionalism: A New Systematic Theorisation", fn. 18..

39 I. Augsberg, *Informationsverwaltungsrecht: Zur kognitiven Dimension der rechtlichen Steuerung von Verwaltungsentscheidungen*, 2014; R. Campos, *Metamorfoses do Direito Global, fn. 15*.

40 I. Augsberg, *Informationsverwaltungsrecht: Zur kognitiven Dimension der rechtlichen Steuerung von Verwaltungsentscheidungen*, fn. 39; R. Campos, *Metamorfoses do Direito Global, fn. 15*.

in the context of the crisis of traditional State regulation due to increasing societal complexity combined with the absorption of State functions by private activities, aimed to connect two dimensions of society: public objectives oriented towards the public interest, and sectoral knowledge from private entities for the implementation of these objectives.[41] As constitutional lawyer Dieter Grimm explains, this new institution of administrative law, situated at the intersection of procedural dimensions, state law, and social complexity, represents the most advanced form of proceduralization[42]. It is a more efficient form of regulation that essentially relies on the collaboration between the regulating state and the actors or societal sectors being regulated.[43]

Perhaps one of the institutions that best illustrates how regulated self-regulation enables the impacts of technology to be addressed through legal norms is the right to the protection of personal data, which will serve as the foundation for the discussion in this essay. We will then analyse self-regulation in the regulatory standards for AI in Europe and Brazil and compare the two approaches.

41 A. Voßkuhle, *Regulierte Selbstregulierung – Zur Karriere eines Schlüsselbegriffs*, in: *Regulierte Selbstregulierung als Steuerungskonzept des Gewährleistungsstaates: Ergebnisse des Symposiums aus Anlaß des 60. Geburtstages von Wolfgang Hoffmann-Riem*, Die Verwaltung Beiheft 4 (2001), p. 197.

42 The model of proceduralization, understood here as the third legal paradigm, differs in terms of the conditions for the production and reproduction of legal normativity in modern society from previous models of state centrality and balancing: "It differs, on the one hand, from the legacy of *quod omnes tangit* in that it does not (solely) concentrate the structures for the production and reproduction of legal normativity within the unity of a national political system. On the other hand, compared to the balancing paradigm, the model of proceduralization does not reduce the conditions for the reproduction of legal normativity to the collision of abstract principles to be resolved within the framework of constitutional adjudication. [...] Proceduralization specifically arises from the bankruptcy, or rather the insufficiency, of the two preceding models, as it incorporates the premises of both paradigms, namely the centrality of the state (*quod omnes tangit*) and the materialization of law in abstract principles mediated by constitutional adjudication (balancing)." G. Abboud; Campos, R., *A Autorregulação Regulada Como Modelo do Direito Proceduralizado*. In: G. Abboud; N. Júnior; R. Campos (Ed.): *Fake News e Regulação*, São Paulo, 2022. For more on this, see D. Grimm, *Regulierte Selbstregulierung in der Tradition des Verfassungsstaats*, in: *Regulierte Selbstregulierung als Steuerungskonzept des Gewährleistungsstaates*, Berlin, 2001,, p. 9.

43 G. Abboud; Campos, R., *A Autorregulação Regulada Como Modelo do Direito Proceduralizado* (Fn. 41).

II. Self-Regulation under the European General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) presents a detailed approach to self-regulation, primarily through the certification mechanisms described in its Articles 42 and 43. This approach, which can be referred to as a form of "regulated self-regulation," represents a combination of traditional self-regulation with stricter state oversight. The GDPR model values the advantages of self-regulation, such as sector-specific knowledge and flexibility, while simultaneously addressing common shortcomings, such as inconsistent application and a lack of effective enforcement.

In connection with the regulation, certification is no longer merely an instrument for organizations to voluntarily declare their compliance, but it has become an important regulatory tool that signals greater commitment and adherence to the standards established by the GDPR.[44] Certifications must be issued by accredited organizations that undergo strict scrutiny and are approved by national data protection authorities. These authorities play a crucial role, as they not only facilitate the process but also actively monitor and enforce the standards set by these entities, ensuring that the certification bodies are competent and well-prepared to assess compliance with the strict requirements of the GDPR.

This integration requires that the certification bodies and their procedures are aligned with the specific criteria of the GDPR, ensuring that they make an effective contribution to the overall data protection ecosystem and improve the transparency of the certification process, as certifications are overseen by data protection authorities. Certified organizations must adhere to high data protection standards, and their compliance is regularly reviewed, meaning continuous monitoring takes place. This helps reduce accountability gaps, which are often observed in purely self-regulatory structures.

In addition, the GDPR's certification process encourages organizations to adopt best practices in data protection by fostering a culture of compliance and continuous improvement, benefiting not only the organizations but also the public and the individuals whose data is processed. By structuring the certification framework, the GDPR effectively bridges the gap between self-regulation and state regulation, as it provides the flexibility and sector-

44 E. Lachaud, *The General Data Protection Regulation and the rise of certification as a regulatory instrument*, in: *Computer Law & Security Review* 34/2 (2018), pp. 244–256.

specific adaptation typical of self-regulation while ensuring that this freedom leaves no room for lax standards or non-compliance. This underscores the GDPR's commitment to maintaining high data protection standards throughout Europe and enhances both organizational accountability and the protection of personal data.

In short, in the GDPR, the regulated self-regulation through certification proposes a balanced approach that leverages the advantages of self-regulation — such as market vision, innovation, and flexibility—while ensuring robust oversight to maintain public trust and protect the rights of individuals. This model can serve as an example for other regulatory frameworks that seek to utilize the benefits of self-regulation without forgoing the oversight and accountability provided by traditional regulatory mechanisms.

III. Self-Regulation in the Brazilian General Data Protection Law (LGPD)

In Brazil, the concept of regulated self-regulation was introduced into the legal framework particularly within the General Data Protection Law (*Lei Geral de Proteção de Dados*, or LGPD), which was heavily inspired by international standards, such as the European Union's General Data Protection Regulation (GDPR).[45] According to Article 50 of the LGPD, controllers and processors responsible for data processing may, within the scope of their powers, individually or through associations, establish rules of good practice and governance. These rules define the conditions for organization, operational procedures, processes — including complaints and requests from data subjects — security standards, technical standards, specific obligations of those involved in data processing, awareness-raising measures, internal monitoring, risk mitigation mechanisms, and other aspects related to the processing of personal data. These rules of good practice and governance can be recognized and disseminated by the National Data Protection Authority (*Autoridade Nacional de Proteção de Dados,* or ANPD) in accordance with Article 50, §3 of the LGPD.

The range of topics that can be addressed within the framework of regulated self-regulation is broad and covers an exemplary spectrum of

45 In the debate surrounding the draft bill for a law on media transparency, which became known as the "Fake News Law," the decision was made to include the institution of regulated self-regulation. For more on this topic, see J. Maranhão; R. Campos, *Exercício de autorregulação regulada das redes sociais no Brasil*. In: Nery, N. Campos; Abboud, Georges (Ed.): *Fake News e Regulação*, São Paulo: RT, 2018.

possibilities that can be explored through this mechanism. These include complaints and petitions from data subjects, which provide individuals with a means to raise concerns or request corrections related to the use of their personal data. Equally important are security standards, which establish minimum requirements for the protection of data against unauthorized access or loss. Technical standards ensure compatibility and security between different systems and technologies. Awareness-raising measures are essential to inform and educate both professionals and the general public about the importance and methods of protecting personal data. Internal monitoring and risk mitigation mechanisms help organizations proactively oversee and adjust their practices to avoid data breaches. In addition to these aspects, other elements related to the processing of personal data are also considered, resulting in a comprehensive and detailed approach to the management and protection of personal information.

By allowing controllers and processors to formulate rules of good practice and governance concerning aspects of personal data processing within their respective areas of responsibility, the law brings together two legal institutions within the regulatory framework of personal data protection: "the ability of the state to recognize non-legislative normative sources, and the voluntary exercise of accountability and self-restraint by these processors, with the role of the ANPD as a security authority being to provide legal certainty and establish guidelines for these multi-stakeholder phenomena."[46]

Since the LGPD gave the ANPD considerable leeway to recognize and publish these rules without specifying the criteria for this authority, in practice there has been an "insufficient use of the mechanism by processors due to a number of questions regarding its operationalization."[47]. There was therefore "a mistrust of the institution, which went so far as to make it opaque, without attracting attention or interest compared to other LGPD topics, even in the academic field."[48]

While, on the one hand, the LGPD has satisfactorily introduced regulated self-regulation, on the other hand, with regard to seals and certifications, there is a need for stronger normative support through regulation by the national data protection authority or a legislative amendment, as this issue

46 Hahn (Fn. 14), p. 11.
47 Hahn (Fn. 14), p. 9.
48 Hahn (Fn. 14), p. 9.

is currently only addressed as a legal basis for international data transfers.[49] The ANPD could act as the accrediting body for seals and certifications on various issues related to LGPD compliance, thus paving the way for impartial audits of processors by properly accredited certifying entities, while ensuring minimal intervention and behaviour-promoting measures from the administration.

D. Regulation of Artificial Intelligence through Self-Regulatory Mechanisms

I. Initial Considerations

The governance of AI brings with it ethical, legal, regulatory, and technical challenges, which have sparked debates about when or whether a legal-regulatory framework is necessary, whether ethical or technical approaches are sufficient, and whether the existing ethical and regulatory frameworks adequately address the impacts of AI.[50] It is evident, however, that trust in AI systems and products is a fundamental criterion for the widespread adoption of AI[51], as "trust is the foundation of societies, economies, and sustainable development," and it is undeniable that "individuals, organizations, and societies will only be able to fully realize the potential of AI if trust in its development, deployment, and use can be established." [52]

In general, two major categories of self-regulatory mechanisms can be distinguished. The first category includes labels, seals, certification systems, quality seals, and trust seals. These are mechanisms that set a specific stan-

49 Chapter V of the LGPD.

50 C. Cath, *Regulierung der künstlichen Intelligenz: Ethische, rechtliche und technische Möglichkeiten und Herausforderungen*, in: *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, v. 376, n. 2133, 2018, available at: https://royalsocietypublishing.org/doi/10.1098/rsta.2018.0080 (accessed on 05.10.2023).

51 European Commission, *Proposal for a Regulation of the European Parliament and of the Council laying down requirements for artificial intelligence. Initial Impact Assessment*, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=PI_COM(2020)3896535&from=EN; European Commission, *White Paper on Artificial Intelligence: A European Approach to Excellence and Trust*, available at: https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf (accessed on 05.10.2023).

52 S. Thiebes / S. Lins / A. Sunyaev, *Vertrauenswürdige künstliche Intelligenz*, in: *Elektronische Märkte* 31 (2021), pp. 447-464, available at: https://link.springer.com/article/10.1007/s12525-020-00441-4 (accessed on 05.10.2023).

dard for AI applications and outline a set of criteria by which that standard is assessed, usually through an audit process. The second category includes codes of conduct and ethics, which can be described as declarations that establish and define requirements or principles that organizations developing or acquiring AI applications must follow. These codes aim to ensure the safe and ethical development and use of these systems, although they generally do not define measurable criteria or involve an audit process.[53]

Labelling initiatives are intended to benefit both consumers and end-users of AI applications as well as the organizations that develop them. For the first group, one of the main goals of these initiatives is to strengthen trust in AI applications by signalling technical reliability and quality[54]. Self-regulatory mechanisms can also enhance competition by creating transparency and comparability between the AI applications available on the market.[55] For companies developing AI applications, one of the main advantages of these initiatives is that they learn how to comply with emerging standards and best practices for a technology like AI[56]. A key aspect shared by most of these initiatives, in line with their intended goals, is the use of an audit process conducted by independent third parties. Similarly, codes of conduct aim to strengthen the trust of end-users and consumers and guarantee good practices in the acquisition and use of AI systems that are safe and ethically sound.[57]

D'Angelo et al. highlight several opportunities that arise from granting seals, codes of conduct, and other self-regulatory mechanisms currently being developed for AI applications. Among the most significant opportu-

53 C. D'Angelo et al., *Labelling initiatives, codes of conduct and other self-regulatory mechanisms for artificial intelligence applications: From principles to practice and considerations for the future*, Santa Monica, CA 2022, available at: https://www.rand.org/pubs/research_reports/RRA1773-1.html (accessed on 05.10.2023).

54 KI.NRW: *Designing Artificial Intelligence Secure and Trustworthy: The next Big Step towards a Certification of AI "Made in Germany"*, February 26, 2021. Accessed on December 8, 2021: https://www.ki.nrw/en/designing-artificial-intelligence-secure-and-trustworthy-the-next-big-step-towards-a-certification-of-ai-made-in-germany/.

55 S. Kelley; Y. Levin; D. Saunders, *A Code of Conduct for the Ethical Use of Artificial Intelligence in Canadian Financial Services*, Smith School of Business, Queen's University, 2018. Accessed on December 8, 2021: https://www.researchgate.net/publication/342168576_A_Code_of_Conduct_for_the_Ethical_Use_of_Artificial_Intelligence_in_Canadian_Financial_Services.

56 C. Galán, *The Certification as a Mechanism for Control of Artificial Intelligence in Europe, European Union*, 2019. Accessed on December 8, 2021: https://ec.europa.eu/futurium/en/system/files/ged/c._galan_phd_-_ai_paper.pdf.

57 D'Angelo et al. (Fn. 53).

nities is the promotion of the ethical development and use of AI products and services, which is crucial given the frequent perception of these systems as opaque. Additionally, these initiatives help build trust in AI products and services. Another important aspect is strengthening the relationships between actors in the AI supply chain during its development and implementation. Such mechanisms are also key to signalling specific standards to companies and end-users in the market, setting market standards, and enhancing global competitiveness[58]. Finally, they propose reintroducing human oversight into technological processes and emphasize the importance of human interaction in technology management.

The challenges associated with self-regulation in AI applications are numerous and multifaceted. First, due to the complexity of AI applications, it is difficult to develop and apply criteria for assessing ethical and legal principles. This complexity also requires the involvement of various stakeholders in the design and implementation of the evaluation. Moreover, the potential costs and effort involved in the evaluation may discourage participation, especially for small companies, which may perceive the process as too expensive or burdensome. In the design and implementation of self-regulation systems, there is a significant conflict between the goal of protecting consumers and promoting innovation and competition in the market. Another challenge is to ensure the legitimacy and accountability of these initiatives through transparent third-party audits. The multitude of different initiatives can confuse both companies and consumers, potentially eroding trust in these measures. Finally, promoting the adoption of voluntary self-regulation mechanisms is challenging, particularly in a competitive environment where compliance with regulations may be seen as a strategic disadvantage.[59]

These challenges highlight the complexity and the need for carefully balanced approaches to ensure that self-regulation efforts are effective and beneficial for both the AI industry and consumers. Self-regulation for AI presents a promising perspective for promoting its ethical and responsible development, and several factors can be considered to strengthen and support this approach. For example, the active involvement of a wide range of stakeholders from different disciplines in the design and development of

58 M. Haataja, *How Certification Promotes Responsible Innovation in the Algorithmic Age*, 2020. Accessed on December 8, 2021: https://bdtechtalks.com/2020/05/28/autonomous-intelligent-systems-certification-ieee/.

59 D'Angelo et al. (Fn. 53).

self-regulation instruments for AI can increase engagement and acceptance of these initiatives, allowing for the inclusion of diverse perspectives and knowledge, which enriches the process. It is also important to recognize that seeking innovative approaches is essential to address the perceived costs and burdens associated with implementing self-regulation mechanisms[60]. Furthermore, innovation provides flexibility and adaptability in the assessment of AI systems and fosters an innovation-friendly environment[61].

II. The European Experience

Although not specified in the European AI Act itself, the European Commission's White Paper on Artificial Intelligence made additional recommendations for the use of voluntary certification systems and seals[62]. In the Commission's initial impact assessment of the AI Act, an EU law to introduce voluntary labelling systems was proposed as a policy option[63]. With the goal of "strengthening user trust in AI systems and promoting the widespread adoption of the technology," the White Paper proposed voluntary labelling systems for low-risk AI, which would "allow economic operators to signal that their AI-based products and services are trustworthy [...] so that users can easily recognize that the relevant products and services meet certain objective and standardized EU-wide norms that go beyond the normally applicable legal obligations."[64] Although participation in the labelling scheme is voluntary, providers who choose to take part must meet certain EU-wide requirements (in addition to existing EU legislation) in order to carry an AI quality mark. The quality seal would demonstrate to the market that the AI application is reliable.

60 Swiss Digital Initiative, *Labels and Certifications for the Digital World: Mapping the International Landscape*, 2021. Accessed on December 8, 2021: https://a.storyblok.com/f/72700/x/73839efcca/attch-1_sdi_initiatives_final.pdf.

61 G. Myers; K. Nejkov, *Developing Artificial Intelligence Sustainably: Toward a Practical Code of Conduct for Disruptive Technologies*, 2020. Accessed on December 8, 2021: https://openknowledge.worldbank.org/bitstream/handle/10986/33613/Developing-Artificial-Intelligence-Sustainably-Toward-a-Practical-Code-of-Conduct-for-Disruptive-Technologies.pdf.

62 European Commission, *White Paper on Artificial Intelligence: A European Approach to Excellence and Trust*, available at: https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf (accessed on 05.10.2023).

63 European Commission, *Proposal for a Regulation of the European Parliament and of the Council laying down requirements for artificial intelligence* (Fn. 51).

64 European Commission, *White Paper on Artificial Intelligence* (Fn. 51).

Based on these proposals, a growing number of voluntary and self-regulatory initiatives for the ethical development of AI have been suggested by stakeholders from the private sector, civil society, as well as academia and politics. For example, the Bertelsmann Foundation has proposed the creation of an ethical quality seal for AI systems.[65] Denmark[66] and Malta[67] have recently published national AI strategies in which they propose a seal and certification program for AI products and services. Several other organizations, such as the All-Party Parliamentary Group on Data Analytics, the Institute of Electrical and Electronics Engineers (IEEE), and the World Economic Forum, have also suggested ideas for AI labelling or certification systems.[68] Most of these initiatives, however, still need to be developed and tested in practice. Similarly, a growing number of codes of conduct for AI are being developed by industry associations, academic and research institutions, corporations, and public sector organizations, such as the one for the British National Health Service (NHS).[69]

The proposed use of seal schemes and codes of conduct for low-risk AI applications is partly based on the implementation of these self-regulatory mechanisms in other industries.[70] Labels and seals are particularly ubiquitous in the food industry, where nutritional values are uniformly color-coded, and the sustainability performance of products is visually verified through standards and seals. In the context of environmental labelling and information regulations, environmental seal schemes have proven use-

65 VDE, Bertelsmann Stiftung. *From Principles to Practice: An interdisciplinary framework to operationalise AI ethics*, available at: https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/WKIO_2020_final.pdf (accessed on 05.10.2023).

66 Danish Government, *National Strategy for Artificial Intelligence*, 2019, available at: https://en.digst.dk/media/19337/305755_gb_version_final-a.pdf (accessed on 05.10.2023).

67 Malta, *Towards an AI Strategy: High-level policy document for public consultation*, 2019, available at: https://malta.ai/wp-content/uploads/2019/04/Draft_Policy_document_-_online_version.pdf (accessed on 05.10.2023).

68 Zeichner, Daniel; Clement-Jones, Tim; Holmes of Richmond, Chris, *An Ethical AI Future: Guardrails & Catalysts to Make Artificial Intelligence a Force for Good*. Policy Connect, June 19, 2023. Available online at: https://www.policyconnect.org.uk/research/ethical-ai-future-guardrails-catalysts-make-artificial-intelligence-force-good, last accessed on: October 9, 2024.

69 GOV.UK, *New code of conduct for artificial intelligence systems used by the NHS*, 2019, available at: https://www.gov.uk/government/news/new-code-of-conduct-for-artificial-intelligence-ai-systems-used-by-the-nhs(accessed on 05.10.2023).

70 D'Angelo et al. (Fn. 53).

ful for harmonizing countries' approaches to environmental criteria and reducing administrative costs, which can lead to an increase in trade with environmentally certified goods.[71]

While these examples are useful comparisons, the differences in labelling within the digital context must be taken into account, including industry-specific issues such as the protection of personal data, the rapid development of technology, and territoriality, which present unique challenges.[72] The same applies to codes of conduct, which, while consistent across all sectors and industries, must be adapted to the specific concerns and characteristics of AI systems. In the case of the European Union, they should meet the requirements for high-risk AI, as proposed in the AI Act.[73]

III. The Brazilian Experience

In the Brazilian context, conversely, AI regulation has almost undergone a pendulum swing, initiated by the Brazilian Strategy for Artificial Intelligence (EBIA), to which Bill 21/2020, largely principle-oriented, was added. On the other hand, Bill 2338/23, the result of the work of a commission of legal experts appointed to address the issue, was largely inspired by the AI Act model and adopts many of its rules. Additionally, a "legal framework for artificial intelligence" in Brazil was the subject of debate by the Senate's internal ad hoc committee on artificial intelligence (*Comissão Temporária Interna sobre Inteligência Artificial*, or CTIA), whose task was to review the projects attached to the final report approved by the commission of legal experts, as well as all new projects that could regulate the issue. From this debate emerged a substitute bill that intends to be a middle ground between the two main approaches that had existed until then. Among the concerns of the new AI bill are topics such as development within the age-

71 M. Klintman, *A Review of Public Policies Relating to the Use of Environmental Labelling and Information Schemes (ELIS)*, in: *OECD Environment Working Papers*, n. 105, available at: https://www.oecd-ilibrary.org/environment/a-review-of-public-policies-relating-to-the-use-of-environmental-labelling-and-information-schemes-elis_5jm0p34bk7hb-en (accessed on 05.10.2023).

72 D'Angelo et al. (Fn. 53).

73 European Commission, *Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts*, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206 (accessed on 05.10.2023).

old dilemma of innovation and regulation, the search for the ideal balance that does not exclude Brazil from the "AI gold rush" while preserving the mitigation of risks inherent in a continental country with many racial and social differences, to name a few.

As for self-regulation, the approach proposed in the CTIA's draft is remarkably integrative and cooperative, aiming to create a governance structure that connects state authorities with self-regulatory bodies. The inclusion of self-regulatory organizations in the National System for Regulation and Governance of Artificial Intelligence (SIA) is a key strategy for implementing a regulatory system that values sector-specific expertise while maintaining the oversight and control necessary to ensure compliance with ethical and legal standards. Article 40 of the draft contains definitions regarding the functioning and composition of the SIA. The text explicitly mentions the involvement of "self-regulatory bodies" as its members, indicating a model where the private sector plays an active role in the creation and implementation of behavioural standards, which can include the establishment of ethical practices, information security, and specific technical standards for the development and application of AI. "Accredited certification bodies" are also mentioned as part of the SIA, suggesting that certification will play a key role in verifying compliance with the standards set by the industry and government regulation. This reflects an approach similar to the "regulated self-regulation" model of the General Data Protection Regulation, where certification is not just a conformity seal but an active regulatory tool that promotes ongoing compliance with regulations and regular evaluations.

As per the system's objectives and foundations, the draft emphasizes the importance of assessing and strengthening the regulatory powers of agencies and regulatory bodies in line with the general guidelines of the responsible authority coordinating the system. This means an effort to align self-regulation standards with broader state regulations, ensuring that AI practices are safe, ethically sound, and responsible. In this context, the system aims for decentralized collaboration between agencies and regulatory bodies at various levels of government (federal, state, district, and municipal), which is essential for a dynamic and cross-sectoral field like AI. Additionally, harmonization with other cross-sectoral regulatory areas, such as antitrust law and consumer protection, is pursued, reflecting a holistic approach to addressing the multidimensional challenges that AI presents.

Article 41 of the draft, in turn, sets out the responsibilities and authorities of the competent body, designated as the coordinating entity of the national regulatory and governance system for artificial intelligence. This provision highlights the fundamental role of this body within the regulatory and governance structure for AI in Brazil, reflecting a governance model that encompasses both regulation and self-regulation, like the one previously discussed in relation to the General Data Protection Regulation (GDPR).

According to the draft, the responsible authority is expected to represent Brazil in international forums on artificial intelligence, ensuring that the country aligns with global practices and standards and can influence the development of international AI regulation. The authority is empowered to issue binding standards in collaboration with other regulatory bodies of the National System for the Regulation and Governance of Artificial Intelligence. These standards cover important aspects such as legally guaranteed rights, transparency requirements in the use of AI systems, certification of systems deemed high-risk, algorithm impact assessments, and procedures for reporting serious incidents. These norms are crucial to ensuring that companies dealing with AI comply with stringent standards, thereby protecting citizens' rights and the integrity of AI systems.

Additionally, the authority is responsible for issuing general guidelines, which are not binding but should orientate the development, implementation, and use of AI systems and shape responsible practices in this sector. The authority may also enter into regulatory agreements with members of the SIA to establish specific rules and coordination procedures, thereby facilitating effective collaboration between different regulatory bodies and AI sectors. Although the authority's involvement in the regulatory processes of other regulatory bodies is not binding, it is crucial to ensuring a coherent approach to AI regulation across various sectors. Furthermore, the authority holds comprehensive normative, regulatory, and sanctioning powers in economic sectors where there is no specific regulatory body or accredited self-regulatory organization, ensuring comprehensive and integrative regulation of AI across all areas of economic activity. In regulatory sandbox environments related to AI, the authority should be informed of activities and can intervene to ensure that experiments align with the goals and principles of the law. This enables controlled innovation and creates a space where new technologies and business models can be tested under regulatory supervision

Article 43 of the draft outlines the functions of the responsible authority within the already mentioned SIA, clarifying how self-regulation, codes of

conduct, and other governance practices are to be promoted and managed in the context of AI in Brazil. The responsible authority is tasked with protecting fundamental rights that may be affected by the use of AI systems and must ensure strict oversight and the implementation of protective measures. Furthermore, the authority is responsible for promoting the adoption of best practices and codes of conduct in the development and use of AI, thereby supporting behavioural standards with a focus on ethics, transparency, and accountability. It is also important that the authority be granted the power to conduct internal audits and mandate independent external audits to verify the compliance of AI systems with legal regulations, ensuring that codes of conduct and self-regulation practices are effective rather than mere formalities. The authority must also promote international cooperation to align Brazilian practices with global best practices. Additionally, it can negotiate compromises to resolve irregularities or legal uncertainties and adapt or enhance codes of conduct as needed. The accreditation of institutions to conduct audits and investigations ensures that the monitoring of AI systems is carried out by qualified entities, which strengthens the self-regulation system. Finally, the authority should be capable of handling anonymous complaints, which is essential for exposing and correcting violations without whistleblowers fearing retaliation.

For the purposes that concern us here, it should be noted that Article 44 of the draft stipulates that all regulations and standards created by the responsible authority must be preceded by a public consultation. This provision aims to ensure transparency and democratic participation in the process of formulating strategies and regulations that affect the management and use of artificial intelligence in Brazil.

E. Final Considerations

As constitutional lawyer Dieter Grimm rightly explains, self-regulation largely depends on the collaboration between the regulating state and the societal actors being regulated.[74] Regulated self-regulation is a promising way to foster the ethical and responsible development of AI while also ensuring the flexibility and adaptability needed for innovation, especially filling a gap within the concept of digital constitutionalism related to the generation of social knowledge. Several factors can be considered to

74 *Grimm* (Fn. 42).

strengthen and support this approach. The active, multidisciplinary participation of diverse stakeholders in designing and developing self-regulation instruments for AI can enhance engagement and acceptance, incorporating a wide range of perspectives and expertise to enrich the process. Additionally, adopting innovative approaches is essential to mitigate the perceived costs and burdens of implementing self-regulation mechanisms.

Instead of pursuing a supposedly universal approach, which can quickly become outdated, it is crucial to consider the diverse knowledge-building processes within today's digital society. The use of self-regulation instruments tailored to specific contexts and use cases encourages voluntary adoption while ensuring flexibility. This approach enables the adaptation of standards to the unique demands of different AI applications, fostering a regulatory environment that safeguards fundamental rights while promoting innovation and development.