VOLUME 10 ISSUE 2 ARTICLES & ESSAYS

University of Bologna Law Review

https://doi.org/10.60923/issn.2531-6133/21439

Received: 18 Apr. 2025 | Reviewed: 27 Nov. 2025 | Accepted: 28 Nov. 2025 | Published: 19 Mar. 2026

The Rise of AI Authorities? A Closer Look at Latin America's Institutional Responses and External Influences

ROCCO SAVERINO*, PABLO TRIGO KRAMCSÁK**, BARBARA DA ROSA LAZAROTTO***

*Rocco Saverino (corresponding author) is Doctoral Researcher at the Research Group on Law, Science, Technology & Society (LSTS) of the VUB Brussels University (Belgium). He holds an LL.B. from the University of Mediterranean Studies in Reggio Calabria (Italy) and an LL.M. from the University of Alicante (Spain). His research focuses on the critical role of Market Surveillance Authorities in enforcing the AI Act and on potential overlaps in cross-regulatory enforcement. He is currently contributing to the project Articulating Law, Technology, Ethics and Politics: Issues of Enforcement and Jurisdiction of EU Data Protection Law under and beyond the General Data Protection Regulation (ALTEP-DP). He is a member of the Management Committee of the Data Protection Law Scholars Network (DPSN).

**Pablo Trigo Kramcsák is Doctoral Researcher at the Research Group on Law, Science, Technology & Society (LSTS) of the VUB Brussels University (Belgium), where he is also a legal researcher at the Cyber and Data Security Lab (CDSL) and a fellow at the Brussels Privacy Hub (BPH). He holds an LL.B. from the Pontifical Catholic University of Chile and holds an LL.M. degree in International Law from the Heidelberg University (Germany) and the University of Chile (Chile). His research focuses on legitimate interest as a lawful basis for processing AI training datasets, addressing legal challenges, risks, and impacts on data subjects' rights and freedoms.

***Barbara da Rosa Lazarotto is Doctoral researcher at the Law, Science, Technology and Society Research Group (LSTS) of the VUB Brussels University (Belgium) and Managing Director of the Brussels Privacy Hub, an academic research centre associated with LSTS. She holds an LLM in Judicial Law from the University of Minho (Portugal). Her research centres on the intersection of data protection and data governance, particularly the secondary use of personal and non-personal data within the EU regulatory framework.

@*Rocco.Saverino@vub.be **Pablo.Rodrigo.Trigo.Kramcsak@vub.be
***Barbara.Da.Rosa.Lazarotto@vub.be
iD *0000-0001-8724-2827 **0000-0003-2385-4722 ***0000-0002-8632-8925

ABSTRACT

Artificial intelligence governance in Latin America is emerging through new legislative proposals that increasingly draw on the European Union's Artificial Intelligence Act. This article asks how Latin American countries are designing artificial intelligence oversight and enforcement mechanisms, and whether they are replicating the European institutional model for supervisory authorities. Existing scholarship has examined the circulation of European regulatory models in data protection law, but it has not yet adequately addressed how that influence operates in the early institutional design of artificial intelligence governance in Latin America.

The article develops a comparative legal analysis of the Ibero-American context, with particular focus on Brazil and Chile, in order to assess how European regulatory templates are received, adapted, and operationalized. It argues that Latin American artificial intelligence regulation is likely to follow a pattern already observed in second-generation data protection reforms: the adoption of broad statutory frameworks inspired by European law, but reshaped by local institutional capacities, budgetary constraints, and regional political economy. The analysis shows that the central dilemma concerns whether to extend the mandate of existing data protection authorities to artificial intelligence or to establish specialized supervisory agencies. Brazil and Chile illustrate two especially significant pathways, given Brazil's regional influence within BRICS and MERCOSUR and Chile's role as an open economy deeply integrated into transnational digital governance networks.

The article contributes to comparative scholarship on artificial intelligence regulation by showing how supervisory design becomes a crucial site of legal translation between European regulatory influence and Latin American institutional realities.

KEYWORDS

A.I. Regulation; Personal Data Protection; Supervisory Authorities; Brussels Effect; Institutional Design

EDITORIAL NOTE

During the editorial process of this article, including submission, peer review, and publication, several legislative proposals and regulatory initiatives discussed in the manuscript evolved, with some being amended or formally adopted. The analysis presented in this article reflects the legal and policy context available at the time of writing and submission. Where possible, the authors have sought to incorporate key developments during revision; however, subsequent legislative changes may have occurred after the completion of the manuscript. The discussion should therefore be understood as reflecting the state of the regulatory framework at the time of the research and drafting process.

TABLE OF CONTENTS

BETWEEN NORM-SETTING AND ALIGNMENT: THE AMBIVALENT GLOBAL ROLE OF THE EU AI ACT

In recent years, the governance of artificial intelligence [hereinafter A.I.] has become a central concern across international arenas. A.I. is not merely a technological advance, but a force that reshapes social, economic, and legal structures. In the global proliferation of A.I. policy documents, these texts reveal the tensions and uncertainties surrounding a technology that provokes both optimism and apprehension.[1]

Governance debates extend across ethical principles, technical standards, legal obligations, and institutional mechanisms of accountability. Like earlier data-driven technologies, A.I. has turned governance design into a contested space where competing interests and models converge. It is worth noting that A.I. governance is closely linked to A.I. safety, as both aim to ensure the development of beneficial A.I.[2] While A.I. safety focuses on technical aspects of A.I. design, A.I. governance concerns the policies, norms, laws, and institutional contexts that shape how A.I. is developed and deployed.[3]

Institutions such as the Organisation for Economic Co-operation and Development [hereinafter O.E.C.D.] and the United Nations Educational, Scientific and Cultural Organization [hereinafter U.N.E.S.C.O.] have contributed to the global discourse on the rapid growth of A.I., with O.E.C.D. developing A.I. Principles (first adopted in 2019 and updated in 2024)[4] and U.N.E.S.C.O. adopting the Recommendation on the Ethics of Artificial Intelligence in 2021.[5] Various U.N. agencies have also developed frameworks for model policies on A.I. development and use.[6] These range from principles promoting trustworthy A.I. to recommendations addressing ethics and human rights safeguards. Although non-binding, these initiatives establish a common vocabulary and set of expectations for A.I. governance, often guiding national and regional regulatory efforts. At this level, the focus is less on prescribing detailed compliance mechanisms and more on fostering convergence around shared values, objectives, and risk-management approaches.

[1] *See generally* Inga Ulnicane et al., *Framing Governance for a Contested Emerging Technology: Insights from AI Policy*, 40 POL'Y & SOC'Y 158, 165 (2021).

[2] *See* ALLAN DAFOE, AI GOVERNANCE: A RESEARCH AGENDA (2018).

[3] *See* Matthijs Maas, *Concepts in Advanced AI Governance: A Literature Review of Key Terms and Definitions*, INSTITUTE FOR LAW AI (Oct., 2023), https://law-ai.org/advanced-ai-gov-concepts/.

[4] OECD, Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449 (May 5, 2019), https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449.

[5] UNESCO, Recommendation on the Ethics of Artificial Intelligence, SHS/BIO/PI/2021/1, (2022), https://unesdoc.unesco.org/ark:/48223/pf0000381137/PDF/381137eng.pdf.multi.

[6] *See* U.N., Chief Executives Board for Coordination (CEB), High-level Committee on Management (HLCM), Framework for a Model Policy on the Responsible Use of Artificial Intelligence in UN System Organizations, CEB/2024/HLCM/28/Add.1/Rev.1, (Oct. 10, 2024).

In contrast to these non-binding frameworks, the Council of Europe's Framework Convention on Artificial Intelligence and Human Rights, Democracy, and the Rule of Law represents the first legally binding international instrument in this field.[7] Opened for signature on the fifth of September 2024, the Convention seeks to ensure that all stages of the A.I. lifecycle, from design and development to deployment and use, adhere to principles of human rights, democratic governance, and the rule of law.

Within this multilateral context, regional regulatory hubs have begun to develop concrete legal frameworks. The European Union has emerged as a key standard-setter, shaping A.I. governance through its comprehensive suite of digital regulations, culminating in the A.I. Act. In Latin America, jurisdictions have pursued significant legislative initiatives, often drawing on European data protection and A.I. principles, yet facing the challenge of integrating these normative approaches with local political and institutional realities. At the national level, countries are experimenting with a combination of comprehensive statutes, sector-specific rules, and administrative guidance, producing a diverse patchwork that reflects varying priorities, technological capacities, and regulatory resources.

The European Commission's own strategy illustrates the depth of this regional legal engineering. Building on the European Data Strategy, the Commission has enacted the Data Governance Act (D.G.A.),[8] the Digital Services Act (D.S.A.),[9] the Digital Markets Act (D.M.A.),[10] the Data Act,[11] and, most recently, the A.I. Act, officially published in the Official Journal of the European Union on the twelfth of July 2024.[12]

The A.I. Act must be understood as part of the European Commission's broader strategy for shaping the digital environment. Although each legislative instrument of the mentioned strategy targets a specific dimension of the digital ecosystem, they are conceptually and functionally interlinked. This interdependence is particularly salient

[7] Council of Europe, *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*, CETS No. 225 (Sept. 5, 2024), https://rm.coe.int/1680afae3c.

[8] Regulation (EU) 2022/868, of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), OJ (L 152) 1.

[9] Regulation (EU) 2022/2065, of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), 2022 O.J. (L 277) 1.

[10] Regulation (EU) 2022/1925, of the European Parliament and of the Council of 14 Sep. 2022 on Contestable and Fair Markets in the Digital Sector and Amending Directives 2019/1937/EU and 2020/1828/EU, 2022 O.J. (L 265) 1.

[11] Regulation (EU) 2023/2854, of the European Parliament and of the Council of 13 Dec. 2023 on Harmonised Rules on Fair Access to and Use of Data and Amending Regulation 2017/2394/UE and Directive 2020/1828/EU, 2023 O.J. (L 2854) 1 (EU).

[12] Regulation (EU) 2024/1689, of the European Parliament and of the Council of 13 June 2024 on Laying Down Harmonised Rules on Artificial Intelligence and Amending Regulations 300/2008/EC, 167/2013/EU, 168/2013/EU, 2018/858/EU, 2018/1139/EU and 2019/2144/EU and 2014/90/EU, 2016/797/EU and 2020/1828/EU, 2024 O.J. (L 1689) 1 (EU).

in A.I., which relies heavily on access to large volumes of data for training, testing, validation, and deployment. In this sense, effective data governance is not merely complementary but foundational to the regulation of A.I.,[13] ensuring consistency, coherence, and legal certainty across the E.U.'s digital regulatory landscape.

The A.I. Act also draws on earlier strategic initiatives. In April 2018, the Commission Communication "Artificial Intelligence for Europe" introduced the European A.I. strategy,[14] an initial approach to the A.I. domain. While presenting itself more as a statement of intent, its holistic approach and recognition of coordinated action between different Member States have allowed it to lay the groundwork for the regulatory future of A.I.[15] in Europe and beyond. Indeed, in its Communication of the eighth of April, the Commission acknowledged the importance of international cooperation in this regard, stating that it "will continue its efforts to bring the Union's approach to the world stage and build a consensus on human-centred AI", further adding that "the European Union have a leadership role in developing international [A.I.] guidelines and, if possible, a related assessment mechanism".[16] From its inception, the A.I. Act was designed with a view to its potential global implications. The A.I. Act applies to A.I. providers and users within the E.U. and extends to non-E.U. actors whose A.I. outputs are deployed in the Union, asserting an extraterritorial scope comparable to that of the G.D.P.R.,[17] which may be reinforced through trade relationships and international cooperation. For these legal instruments to be effective, they must bind non-European actors to European regulatory frameworks, either through local establishment, representation, or extraterritorial enforcement mechanisms.[18] In this context, the A.I. Act has the potential to shape global approaches to the development and deployment of A.I. systems.[19]

[13] *See* Marijn Janssen et al., *Data Governance: Organizing Data for Trustworthy Artificial Intelligence*, GOV'T INFO. Q., July 2020, at 1.

[14] Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, Artificial Intelligence for Europe, COM (2018) 237 final (Apr. 25, 2018).

[15] Behind this vision are three pillars: i) increasing both public and private investment in A.I., ii) preparing for economic change, and iii) ensuring a European ethical and legal framework. To do this, an Expert Group on A.I. is created to lay down guidelines on trustworthy AI development. *See* Nathalie A. Smuha, *The EU Approach to Ethics Guidelines for Trustworthy Artificial Intelligence*, 20 COMPUT. L. REV. INT'L 97 (2019) (Ger.).

[16] *Supra* note 14.

[17] *See generally* Mateo Aboy et al., *Navigating the EU AI Act: Implications for Regulated Digital Medical Products*, NPJ DIGIT. MED., Sep. 2024, at 1, 3.

[18] *See* VAGELIS PAPAKONSTANTINOU & PAUL DE HERT, THE REGULATION OF DIGITAL TECHNOLOGIES IN THE EU: ACT-IFICATION, GDPR MIMESIS AND EU LAW BRUTALITY AT PLAY 112 (2025).

[19] *See* CHARLOTTE SIEGMANN & MARKUS ANDERLJUNG, THE BRUSSELS EFFECT AND ARTIFICIAL INTELLIGENCE: HOW EU REGULATION WILL IMPACT THE GLOBAL AI MARKET 5 (2022).

This international focus reflects the E.U.'s ambition to establish itself as a global leader, drawing from its past influence on digital regulation beyond its borders, including international agreements and the Brussels Effect,[20] where its regulations set a *de facto* standard globally.[21] The Brussels Effect "detaches globalisation from the idea of deregulation and the race to the bottom",[22] i.e., the idea that countries lower their regulatory standards to improve their relative competitive position in the global economy.[23] Instead, it describes a form of unilateral regulatory globalisation grounded in the E.U.'s market size, institutional capacity, preference for stringent rules, access to inelastic consumer markets, and the non-divisibility of standards.[24] In the case of the A.I. Act, these dynamics may be reinforced by a first-mover advantage.[25]

While many jurisdictions in the majority world often align with E.U. standards to facilitate trade, attract investment, or gain legitimacy in the international arena, the adoption of such standards is rarely straightforward.[26] In Latin America, for example, countries may selectively incorporate aspects of E.U. regulations while adapting them to local political priorities, administrative capacities, and social expectations. This can involve modifying compliance requirements to reflect institutional constraints, prioritising certain rights or protections over others, or integrating regional norms and principles, such as those emerging from inter-American human rights frameworks.[27]

The interest in A.I. governance has resonated beyond the E.U. As noted, international frameworks such as those developed by the O.E.C.D. and U.N.E.S.C.O. provide guiding principles for A.I., each reflecting different emphases and constituencies. While the O.E.C.D. primarily represents high-income economies,[28] U.N.E.S.C.O. brings a more inclusive perspective focused on ethics and human rights.

[20] *See* ANU BRADFORD, THE BRUSSELS EFFECT: HOW THE EUROPEAN UNION RULES THE WORLD (2020).

[21] *See* Marco Almada & Anca Radu, *The Brussels Side-Effect: How the AI Act Can Reduce the Global Reach of EU Policy*, 25 GERMAN L.J. 646 (2024) (U.K.).

[22] Interview by Groupe d'Études Géopolitiques with Anu Bradford, Professor of Law, Columbia Univ. (2021) (*The European Union in a Globalised World: The "Brussels Effect"*), https://geopolitique.eu/en/articles/the-european-union-in-a-globalised-world-the-brussels-effect/.

[23] Anu Bradford, *Exporting Standards: The Externalization of the EU's Regulatory Power Via Markets*, 42 INT'L REV. L. & ECON. 158 (2015).

[24] *Id.* at 161.

[25] Siegmann & Anderljung *supra* note 19, at 11.

[26] *See* Patricia Boshe & Carolina Goberna Caride, *Is the Brussels Effect Creating a New Legal Order in Africa, Latin America and the Caribbean?*, 2023 TECH. & REGUL. 12.

[27] *See* Organization of American States (OAS), Updated Principles on Privacy and Personal Data Protection (2021), https://www.oas.org/en/sla/iajc/docs/Publication_Updated_Principles_on_Privacy_and_Protection_of_Personal_Data_2021.pdf.

[28] In the Latin American region, OECD engagement encompasses the member states of Chile, Colombia, Costa Rica, and Mexico, along with Argentina, Brazil, and Peru, which are undergoing accession processes. *See Latin America and the Caribbean*, O.E.C.D. (2025), https://www.oecd.org/en/regions/latin-america-and-the-caribbean.html.

These frameworks have helped set the stage for the E.U.'s A.I. Regulation, which contributes to the expanding reach of the Brussels Effect in the sector.[29] The A.I. Act's influence is likely to emerge more through emulation by other countries than through its direct legal force.[30] Nevertheless, debate continues over the extent to which the A.I. Act will achieve meaningful global impact.[31]

The effectiveness of A.I. Regulation increasingly depends on a coherent, coordinated, and adequately resourced governance framework, especially given the growing demand for harmonised regulatory practices in the digital domain.[32] While the E.U.'s A.I. Act presents a comprehensive and ambitious hybrid framework (primarily focused on product safety and standardisation, with some provisions addressing fundamental rights),[33] it remains deeply rooted in Europe's political, legal, and institutional landscape. Its complexity and resource demands make it an unlikely universal template. Nevertheless, it provides some lessons that can inform and inspire diverse regulatory models elsewhere.[34]

This institutional flexibility illustrates the E.U.'s effort to reconcile unity with subsidiarity, preserving coherence while accommodating national administrative traditions. Such adaptability, however, carries costs: heightened oversight, greater operational complexity, and coordination demands that vary across Member States. Centralised or resource-constrained systems may experience implementation difficulties. In this context, the possibility for Member States to introduce additional safeguards for the use of A.I. by public authorities further illustrates the tension, as it could generate uneven levels of protection across Europe.[35] Similar pressures for differentiation shaped the legislative process itself, where sustained lobbying by big tech, industry, and Member States drove significant carve-outs and concessions in the final text of the A.I. Act.[36] Rather than a one-size-fits-all model, it seems to offer, in theory, a more balanced approach, particularly regarding enforcement powers and

[29] *See* Bradford, *supra* note 20, at 12.

[30] *See* Graham Greenleaf, *The 'Brussels Effect' of the EU's 'AI Act' on Data Privacy Outside Europe*, 171 Priv. L. & Bus. Int'l Rep. 1 (2021) (Austl.).

[31] *See* Almada & Radu, *supra* note 21, at 2.

[32] *See* Claudio Novelli et al., *A Robust Governance for the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities*, 16 Eur. J. Risk Regul. 566 (2025) (U.K.).

[33] *See* Oskar J. Gstrein, Noman Haleem & Andrej Zwitter, *General-Purpose AI Regulation and the European Union AI Act*, Internet Pol'y Rev., Aug. 2024, at 1 (Ger.).

[34] *See* Marco Almada, *The EU AI Act in a Global Perspective*, Handbook on the Global Governance of AI (Furendal & Lundgren eds., Edward Elgar, forthcoming 2025), https://ssrn.com/abstract=5083993.

[35] *See* Nicoletta Rangone & Luca Megale, *Risks Without Rights? The EU AI Act's Approach to AI in Law and Rule-Making*, 16 Eur. J. Risk Regul. 1082, 1096 (2025) (U.K.).

[36] *See* Raluca Csernatoni, *The EU's AI Power Play: Between Deregulation and Innovation*, Carnegie endowment for int'l peace (May 20, 2025), https://carnegieendowment.org/research/2025/05/the-eus-ai-power-play-between-deregulation-and-innovation.

institutional structure.[37] For global observers, it could function more as a benchmark than a blueprint.

Given these complexities, the international influence of the E.U.'s A.I. Act remains uncertain. While its regulatory framework may inform global A.I. governance debates, its broader applicability hinges on whether other jurisdictions can reconcile the A.I. Act's approach with their systems. As countries grapple with their unique A.I. governance challenges, they face a critical choice: adopt elements of the E.U. model, tailor it to their context, or craft entirely new frameworks aligned with their priorities. Ultimately, the E.U.'s impact on global A.I. Regulation may depend less on the direct uptake of the A.I. Act and more on its ability to catalyse a broader dialogue, one that translates its core principles into adaptable foundations for convergence, rather than rigid templates for replication.

A critical element of A.I. governance is the institutional dimension: who oversees, who enforces, and with what authority and resources. Strong institutions do more than transmit rules: they determine whether regulation is effective. Weak or fragmented oversight can render even the most sophisticated frameworks ineffective. At the same time, well-designed and empowered bodies can ensure that A.I. governance operates not only in theory but in practice. It is precisely this institutional component—its design, capacities, and operational dynamics—that constitutes the central focus of this study.

1. GOVERNANCE FLEXIBILITY IN THE E.U. A.I. ACT: TAILORING INSTITUTIONAL MODELS TO NATIONAL REALITIES

The governance of A.I. at the global level remains fragmented across multiple international initiatives and regional frameworks. In addition to what was already mentioned above about the O.E.C.D. principle and the U.N.E.S.C.O. Recommendations,[38] the United Nations has recently established two key mechanisms for global A.I. governance: the Independent International Scientific Panel on A.I. and the Global Dialogue on A.I. Governance.[39] The Scientific Panel on A.I. will be composed of forty

[37] *See supra* note 33, at 14 (Ger.).

[38] *See supra* notes 4 and 5.

[39] *See* G.A. Draft Res. 79/118 (Aug. 18, 2025).

experts to assess A.I. risks and opportunities, and as stated by the UN Secretary-General, "will serve as a crucial bridge between cutting-edge [A.I.] research and policymaking".[40]

At the regional level, diverse approaches are observed. The E.U. adopted a more precautionary stance towards A.I. governance, as exemplified by the classification of risk levels and the implementation of stricter oversight on high-risk A.I. applications through the A.I. Act. Conversely, the United States [hereinafter U.S] predominantly relies on a market-driven regulatory framework, emphasising voluntary standards and self-regulation.[41]

The situation for Asia is constantly evolving due to a shift from soft to hard regulation, where the existing internet governance framework profoundly influences the A.I. governance.[42] Even though Europe was the first to adopt a comprehensive regulation on A.I., China was the first global superpower to specifically regulate generative A.I. involving multiple agencies, with the Cyberspace Administration of China playing a pivotal role alongside the Ministry of Information and Industry Technology.[43] Remaining in the context of governmental agencies and broadening the vision to the U.S., it can be noted that the agency-level implementation is the critical bottleneck in U.S. A.I. governance due to a lack of technical expertise, resource constraints, and leadership gaps.[44] The discourse on A.I. governance in Latin American countries, which forms the core of this study, particularly regarding the role of competent authorities in enforcing A.I. regulations, will be discussed further in the following sections. In this Section, we will keep the analysis focused on the E.U. approach, highlighting the current situation in specific E.U. Member States.

The A.I. Act's requirement for national enforcement bodies introduces three distinct institutional design paths: the creation of new, dedicated A.I. agencies; the designation of existing bodies; or the establishment of hybrid "competence centres" that combine centralised regulatory expertise with sector-specific knowledge.[45] These

[40] Press Release, United Nations, *Secretary-General Welcomes General Assembly Decision to Establish New Mechanisms Promoting International Cooperation on Governance of Artificial Intelligence*, UN Meetings Coverage and Press Releases sg/sm/2776 (Aug. 26, 2025), https://press.un.org/en/2025/sgsm22776.doc.htm.

[41] *See* Vikram Kulothungan & Deepti Gupta, *Towards Adaptive AI Governance: Comparative Insights from the U.S., EU, and Asia*, Arxiv (Apr. 1, 2025), http://arxiv.org/abs/2504.00652.

[42] *See* Jian Xu, Terence Lee & Gerard Goggin, *AI Governance in Asia: Policies, Praxis and Approaches*, 10 Commc'n Rsch. & Prac. 275 (2024) (Austl.).

[43] *See generally* Matt Sheehan, *China's AI Regulations and How They Get Made*, 24 Horizons: J. Int'l Rels. & Sustainable Dev. 108 (2023) (China); *see also* Hunter Dorwart et al., *Preparing for Compliance: Key Differences between EU, Chinese AI Regulations*, IAPP (Feb. 5, 2025), https://iapp.org/news/a/preparing-for-compliance-key-differences-between-eu-chinese-ai-regulations.

[44] *See* Christie Lawrence, Isaac Cui & Daniel Ho, *The Bureaucratic Challenge to AI Governance: An Empirical Assessment of Implementation at U.S. Federal Agencies*, 2023 AIES '23: Procs. 2023 AAAI/ACM Conf. on AI, Ethics, and Soc'y 606 (Can.).

[45] *See* Novelli et al., *supra* note 32, at 4.

alternatives not only reflect the layered and complex nature of E.U. governance but also underscore the significant challenges involved in translating the A.I. Act's multifaceted architecture to jurisdictions outside the E.U., due to structural differences among the various approaches taken globally to govern A.I. Nevertheless, this fragmentation could "pose challenges to global interoperability, ethical coherence, and policy coordination".[46]

One of the critical issues currently being debated in Europe is whether competent A.I. authorities will comprise the already established D.P.As. in each Member State or whether new regulatory agencies will need to be created to address the unique demands posed by A.I. technologies. In this regard, it is questioned whether, while D.P.As. "are well-versed in privacy issues", they "might not fully address A.I.'s broader impacts",[47] which include aspects such as algorithmic bias, accountability for A.I.-driven decisions, and the societal consequences of widespread A.I. deployment. This has raised a further question on whether D.P.As. should enforce the A.I. Act or not.[48] However, there is currently no standard approach to navigating these complexities, as we will explore in the subsequent paragraphs of this Section. In particular, we will focus on three countries in Europe (France, Italy, and Spain), whose approaches have differed since the first proposal of the E.U. A.I. Act was published in 2021. Indeed, the relevance of analysing Spain reside in its idea of establishing a new agency competent for A.I.; Italy, because of the significant actions of the Italian D.P.A. against A.I. systems even before the A.I. Act was officially published,[49] as well as the attempt to convince Italian government of being the most appropriate authority to deal with A.I. systems (see below); and France due the idea of the same Government to re-organise the current French D.P.A. also for A.I. matters.

The Council of State in France recommended maintaining the French data protection authority, *Commission Nationale de l'Informatique et de les Libertés* [National Commission of Information Technology and Freedoms] [hereinafter C.N.I.L.], as a key player in regulating A.I. A study, published on the thirtieth of August 2022,[50] proposed comprehensive reforms to transform C.N.I.L. into a national regulatory body responsible

[46] *See* Kulothungan and Gupta, *supra* note 41.

[47] *See id.*

[48] *See* Joanna Mazur, Claudio Novelli & Zuzanna Choińska, *Should Data Protection Authorities Enforce the AI Act? Lessons from EU-Wide Enforcement Data* (June 12, 2025), https://papers.ssrn.com/abstract=5290513.

[49] *See* Garante per la protezione dei dati personali, *Intelligenza artificiale: il Garante blocca ChatGPT. Raccolta illecita di dati personali. Assenza di sistemi per la verifica dell'età dei minori*, Garante Privacy (Mar. 31, 2023) https://www.garanteprivacy.it:443/home/docweb/-/docweb-display/docweb/9870847.

[50] Le Conseil d'État, *Intelligence artificielle et action publique: construire la confiance, servir la performance*, Conseil d'État (Aug. 31, 2022), https://www.conseil-etat.fr/publications-colloques/etudes/intelligence-artificielle-et-action-publique-construire-la-confiance-servir-la-performance (Fr.).

for overseeing A.I. systems, including those used in the public sector. The authority's focus would be on protecting fundamental rights and liberties, promoting innovation, and ensuring public efficiency. In the E.U.'s regulatory framework governing A.I., the C.N.I.L. is set to play a comprehensive role, with responsibilities in data protection and oversight of A.I. systems. Its mission also involves significant coordination among regulatory bodies and other stakeholders involved in advancing AI systems. This model reflects a realignment of an existing agency rather than the establishment of a new one, acknowledging the intrinsic interrelationship between A.I. and personal data.

In Italy, on the other hand, the Data Protection Authority [*Garante per la protezione dei dati personali*] (Garante), sought to persuade the Government of the advantages in terms of both time and resources in assigning it responsibility in the field of A.I. It tried to do that by highlighting the close connection between data and A.I., as well as the independence that characterises the D.P.A.s, enshrined in Article 16 of the Treaty on the Functioning of the European Union [hereinafter T.F.E.U.] and Article 8 of the Charter of Fundamental Rights of the EU [hereinafter C.F.R.U.E.].[51] However, the Government submitted a proposal for a national law on A.I. [hereinafter Draft Law],[52] in which specific provisions are related to national competent authorities under the A.I. Act, distinct from the Garante. Indeed, Article 18 of the Draft Law identifies the *Agenzia per l'Italia Digitale* [Agency for Digital Italy] [hereinafter Ag.I.D.][53] and the *Agenzia Nazionale per la Cybersicurezza* [National Agency for Cybersecurity] [hereinafter A.C.N.] as the national competent authorities for A.I.,[54] two authorities with different roles and functions. In practice, Ag.I.D. is responsible for promoting innovation and the development of artificial intelligence, except for cybersecurity, the promotion of which will be the responsibility of A.C.N.[55] This latter, given its role as a cybersecurity agency, will be responsible for the oversight, including inspection and sanctioning activities, of artificial intelligence systems.[56] The governmental nature of these two agencies is clearly defined in paragraph 2 of Article 18, which outlines the coordination with other authorities under the Coordination Committee at the Presidency of the Council of Ministers. Furthermore, the information provided on Ag.I.D.'s website unambiguously

[51] Garante per la protezione dei dati personali, *Segnalazione al Parlamento e al Governo sull'Autorità per l'I.A.*, GPDP (Mar. 25, 2024), https://www.gpdp.it:443/web/guest/home/docweb/-/docweb-display/docweb/9996493 (It.).

[52] *See Disegno di Legge - Disposizioni e delega al Governo in materia di intelligenza artificiale*, (2024), Senato https://www.senato.it/service/PDF/PDFServer/DF/437373.pdf (It.).

[53] Trans. EN: Agency for Digital Italy.

[54] Trans. EN: Agency for National Cybersecurity.

[55] *See* Disegno di Legge - Disposizioni e delega al Governo in materia di intelligenza artificiale, *supra* note 52, article 18.1 (a).

[56] *Id.* article 18.1 (b).

identifies it as the Italian government agency responsible for the governance of A.I.[57] While Article 18(3) explicitly states that "the competencies, tasks, and powers of the [*Garante*] for the protection of personal data shall remain unaffected", this provision did not meet the [*Garante's*] anticipated outcomes before the official proposal of the Draft Law in Italy.

Among European countries, Spain has historically exerted significant influence and plays an important role in shaping regulatory developments in Latin America.[58] Spain has pioneered a distinct approach regarding its A.I. national competent authority: *Agencia Española de Supervisión de la Inteligencia Artificial* [Spanish Agency for the Supervision of Artificial Intelligence] [hereinafter A.E.S.I.A.].[59] The establishment of the A.E.S.I.A. in Spain officially commenced with Law 22/2021 of 28 December, concerning the General State Budget for 2022.[60] This law called upon the government to create a special agency through legislation. Subsequently, the constitutive Statute was approved with the passing of Royal Decree No. 729 on 22nd August 2023 (Statute),[61] and the Governing Council was constituted in December 2023.[62] It stands out as the first country to establish a legal framework for an AI authority operating independently of the D.P.A. This authority is envisioned as an agency that maintains a direct line of communication with the government. Indeed, all A.E.S.I.A.'s Governing Council members, except one, are linked to a Ministry.[63] Additionally, the President of A.E.S.I.A. is the Secretary of State for Digitalisation and Artificial Intelligence[64] and the Director of A.E.S.I.A. is effectively

[57] "*The Agency for Digital Italy (AgID) is the technical agency of the Presidency of the Council of Ministers that guarantees the achievement of the objectives of the Italian digital agenda, coordinating all Italian public admnistrations".* See the full definition https://www.agid.gov.it/en/agency.

[58] *See generally* Alexandre Veronese et al., *The Influence of European Union Personal Data Protection Standards in Latin America From the Perspective of Social Actors and Latin American Authorities*, UNIO - EU L.J., Dec. 20, 2023, at 118 (Port.). The European model of data privacy has been actively advanced in Latin America through the Ibero-American Data Protection Network, with Spain playing a key role in this process. On this matter, see Arturo J. Carrillo & Matías Jackson, *Follow the Leader? A Comparative Law Study of the EU's General Data Protection Regulation's Impact in Latin America*, 16 ICL J. 177, (2022) (Ger.). Spain is both a member of the Ibero-American Data Protection Network and serves as its Permanent Secretariat. *See also* Países RIPD, Red Iberoamericana de Proteccion de Datos, https://www.redipd.org/la-red/integrantes/paises.

[59] Trans. EN: Spanish Agency for the Supervision of Artificial Intelligence.

[60] Agencia Estatal Boletín Oficial del Estado, BOE-A-2021-21653 Ley 22/2021, de 28 de Diciembre, de Presupuestos Generales Del Estado Para El Año 2022, https://www.boe.es/buscar/act.php?id=BOE-A-2021-21653 (accessed May 2, 2024).

[61] Real Decreto 729/2023, de 22 de agosto, por el que se aprueba el Estatuto de la Agencia Española de Supervisión de Inteligencia Artificial, [Royal Decree 729/2023 of Aug. 22 approving the Statute of the Spanish Agency for Supervision of Artificial Intelligence], BOE-A-2023-18911 (Spain).

[62] *Se Constituye El Consejo Rector de La Agencia Española de Supervisión de La Inteligencia Artificial* [*The Governing Council of the Spanish Agency for the Supervision of Artificial Intelligence Is Constituted*], Gobierno de España. Ministerio de Economía, Comercio y Empresa, https://portal.mineco.gob.es/en-us/comunicacion/Pages/071223_Se_constituye_Consejo_Rector_Agencia_Espanola_Supervision_IA.aspx (last visited May 3, 2024) (Spain).

[63] Real Decreto 729/2023, art. 15 of the Statute.

[64] *Id., article 12.*

considered a General Director of the State Administration.[65] Thus, similar to the Italian agency, Spain intends to regulate and govern A.I. through government intervention. The reasons why Spain acted in this way also lay in the fact that the establishment of A.E.S.I.A. was strategically aligned with its E.U. Council Presidency in the second half of 2023.[66] The Spanish presidency made finalising the A.I. Act one of its main priorities, and having an established A.I. regulatory authority enhanced Spain's credibility and influence in the negotiations.

Despite the different actions taken at the national level as observed above, it is crucial to recognise the emphasis placed by some [Data Protection Authorities] [hereinafter D.P.A.s] on the independence of A.I. regulatory bodies (i.e., Italy). These authorities argue that protecting fundamental rights must be the highest priority, necessitating impartial A.I. governance.[67] This perspective highlights the need for AI regulation to prioritise safeguarding fundamental rights, ensuring that A.I. authorities operate independently and effectively in this role.

Therefore, the insistence on the independence of A.I. regulatory bodies reflects the essential goal of protecting fundamental rights in A.I. governance. However, A.I. governance also implies government involvement in regulating AI, which is fundamentally linked to their responsibility to govern A.I. effectively, with consequences for their economic development in both the E.U. and international markets. *De facto*, the reference to national competent authorities in Article 70 of the A.I. Act pertains to Market Surveillance Authorities [hereinafter M.S.A.s] and Notifying Authorities. These authorities are more closely connected to market regulation and play a relevant role in the development of the internal market and the free movement of goods.[68] Indeed, their role is not new in EU Regulations, given that they are the primary authorities for product safety regulation,[69] and the A.I. Act could be considered a medley of fundamental rights

[65] *Id., article 23.*

[66] *See* European Parliament Press Release, Spanish Presidency debriefs EP committees on priorities (Sept. 8, 2023), https://www.europarl.europa.eu/news/it/press-room/20230904IPR04608/spanish-presidency-debriefs-ep-committees-on-priorities.

[67] *See* European Data Protection Supervisor (EDPS) and European Data Protection Board (EDPB), Joint Opinion 5/2021 on the Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) (June 18, 2021), https://www.edps.europa.eu/node/7140_en. *See also*, European Data Protection Board (EDPB), Statement 3/2024 on Data Protection Authorities' Role in the Artificial Intelligence Act Framework (July 16, 2024), https://www.edpb.europa.eu/system/files/2024-07/edpb_statement_202403_dpasroleaiact_en.pdf.

[68] To have complete overview of the EU product rules and the roles of competent authorities involved, *see* Commission Notice, *The 'Blue Guide' on the implementation of EU product rules 2022*, 2022 O.J. (C 247).

[69] Also in the context of the AI Act, Art. 3 defines MSAs as "the national authority carrying out the activities and taking the measures pursuant to Reg. (EU) 2019/1020", i.e., Reg. (EU) 2019/1020 of the European Parliament and of the Council of June 20, 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No. 765/2008 (EU) No. 305/2001, 2019 O.J. (L 169) 1.

and product safety regulation,[70] taking into account its legal basis, Articles 16 and 114 T.F.U.E. Although the focus of this study is mainly on the strict connection between data protection and AI regulations, and consequently on the role of D.P.A.s in AI regulations in the E.U. and in Latin American countries, the relevance of this aspect deserves brief mention.

2. LATIN AMERICA'S RECEPTION OF THE EUROPEAN DATA PROTECTION MODEL: A PRECEDENT FOR GOVERNING DATA-DRIVEN TECHNOLOGIES

Data-governance regulations are central in the discourse and formulation of legal frameworks governing data-driven technologies, particularly A.I.[71] These frameworks lay down the legal foundations that define the conditions under which data may be collected, processed, and used, fostering responsible and trustworthy technological developments. Within this broader governance landscape, data protection regulations establish the legal baseline to ensure A. I systems handling personal data operate fairly, transparently, and accountably, while addressing the risks of discrimination, manipulation, and pervasive surveillance arising from the integration of A.I. and big data, including A.I.-driven inferences and profiling.[72]

The governance of emerging technologies depends on data-protection regulations that function as a fundamental, technology-neutral framework, meaning that the same regulatory principles apply across different technologies and prevent the creation of isolated regulatory silos.[73] Whether applied to A.I., big data analytics, or other digital systems, these regulations set out principles and safeguards that guide both the design and deployment of data-driven tools. These baseline standards render data protection indispensable for governing innovation and maintaining a careful balance between technological advancement and the protection of individual rights.

[70] *See* Marco Almada & Nicolas Petit, *The EU AI Act: A Medley of Product Safety and Fundamental Rights?*, Robert Schuman Centre for Advanced Studies Research Paper No. 2023/59 (Oct. 18, 2023), https://dx.doi.org/10.2139/ssrn.4308072.

[71] *See* Stefaan Verhulst & Friederike Schüür, *Interwoven Realms: Data Governance as the Bedrock for AI Governance*, MEDIUM (Nov. 20, 2023), https://medium.com/data-policy/interwoven-realms-data-governance-as-the-bedrock-for-ai-governance-ffd56a6a4543.

[72] *See* Giovanni Sartor & Francesca Lagioia, *The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence*, European Parliamentary Research Service (June 2020), https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf.

[73] *See* Winston J. Maxwell & Marc Bourreau, *Technology Neutrality in Internet, Telecoms and Data Protection Regulation*, 21 COMPUT. & TELECOMM. L. REV. 1, 1 (2015).

As A.I. systems increasingly rely on large-scale, varied datasets for training and decision-making, ensuring their design and operation align with established data protection principles becomes ever more pressing. Core principles such as lawfulness, purpose limitation, data minimisation, transparency, and accountability act as essential safeguards against the risks associated with A.I. models, many of which stem from how data is collected, processed, and used.[74] In this context, data-processing rules are a structural and normative cornerstone of A.I. regulations. Alignment between A.I.-specific regulatory frameworks and pre-existing data protection regimes is indispensable,[75] not only to guarantee legal certainty but also to uphold individual rights and support the responsible development of emerging technologies.

Data protection laws in Latin America have been shaped by two interrelated factors: the region's political history[76] and the influence of European data protection sources and regulatory frameworks,[77] including those of the Council of Europe. Historical experiences with authoritarianism and the misuse of personal information created an acute awareness of the need to protect individual privacy, establishing a political and social context in which data protection became a pressing concern.[78] At the same time, European norms, first embodied in the Data Protection Directive[79] and later reinforced through the G.D.P.R.,[80] exerted a strong transnational influence known as the Brussels Effect. This influence provided both a practical template and a normative

[74] *See* Information Commissioner's Office, *Regulating AI: The ICO's Strategic Approach* (2024), https://ico.org.uk/media2/migrated/4029424/regulating-ai-the-icos-strategic-approach.pdf.

[75] *See* Belgian Data Protection Authority, *Artificial Intelligence Systems and the GDPR: A Data Protection Perspective* (Dec. 2024), https://www.autoriteprotectiondonnees.be/publications/artificial-intelligence-systems-and-the-gdpr—a-data-protection-perspective.pdf.

[76] Data privacy has long been sensitive in Latin America, where histories of authoritarian rule have allowed governments to intrude under the guise of national security. *See* Luisa Parraguez Kobek & Erik Caldera, *Cyber Security and Habeas Data: The Latin American Response to Information Security and Data Protection,* 24 Oasis 109 (2016).

[77] *See* Carrillo & Jackson, *supra* note 58, at 178.

[78] The legacy of totalitarian regimes led to the incorporation of the endemic Habeas Data rights into many South American constitutions. Habeas Data, which grants individuals the right to access, correct, and update their personal data, was adopted as a democratizing tool to counter authoritarian regimes. *See* Andrés Guadamuz, *Habeas Data vs. the European Data Protection Directive*, J. Info. L. & Tech., Nov. 2001, at 1. *See* Katitza Rodriguez & Veridiana Alimonti, *A Look-Back and Ahead on Data Protection in Latin America and Spain*, Elec. Frontier Found. (Sept. 21, 2020), https://www.eff.org/deeplinks/2020/09/look-back-and-ahead-data-protection-latin-america-and-spain. The Brazilian Constitution inaugurated habeas data in the Global South, responding to the secrecy and arbitrariness with which the dictatorship collected, stored, and used personal data. On this matter *see* Marc T. Gonzalez, *Habeas Data: Comparative Constitutional Interventions from Latin America Against Neoliberal States of Insecurity and Surveillance,* 90 Chi.-Kent L. Rev. 641, 651 (2015).

[79] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281).

[80] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 2016 O.J. (L119) 1.

benchmark, guiding Latin-American countries in designing legal frameworks that align domestic privacy protections with internationally recognised principles and fundamental rights.[81]

This European influence was not abstract. It materialised through the E.U.'s harmonised framework, beginning with Directive 95/46/EC (1995),[82] which established the first comprehensive system for regulating the collection, processing, and transfer of personal data across Member States. Harmonising standards facilitated cross-border data flows within the E.U. single market and provided a model that influenced emerging data protection frameworks in other regions, including Latin America.[83] The adoption of European-style comprehensive data protection laws in the region unfolded in two waves. The first followed the 1995 Data Protection Directive, with Chile (1999), Argentina (2000), and Paraguay (2000) enacting legislation. The second wave came in the next decade, as Uruguay (2008), Mexico (2010), Costa Rica (2011), Peru (2011), Nicaragua (2012), and Colombia (2012) introduced new laws.[84]

Council of Europe's Convention 108,[85] the first binding international treaty on data protection, has also significantly influenced Latin American data protection.[86] For countries with limited resources and experience in privacy, the Convention has offered essential guidance and contributed to the strengthening of legal frameworks and governance across the region.[87] In this context, three Latin-American countries (Mexico,

[81] Certain Latin American countries have recognised data protection as a stand-alone right from the right to privacy. For example, the Mexican Constitution enshrines the right to privacy in Article 16, paragraph 1, and the right to data protection in paragraph 2. In Chile, Law No. 21.096, enacted in 2017, amended Article 19, No. 4 of the Constitution to establish the protection of personal data as an independent fundamental right. Similarly, the Brazilian Constitution guarantees the right to privacy and private life in Article 5, section X, along with a right to data protection in section LXXIX.

[82] Directive 1995/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281).

[83] Parraguez Kobek & Caldera, *supra* note 76, at 114 . It should be noted that this process was not homogeneous. Brazil lacked a comprehensive framework for protecting personal data before its General Data Protection Law No. 13,709/2018 (Lei Geral de Proteção de Dados or LGPD) came into effect on August 16, 2020. Its data protection strategy was mainly siloed, *cf.* Pablo Trigo Kramcsák, *Personal Data Protection and Data Transfer Regulation in Brazil* 1-29, 7 (Brussels Priv. Hub, Working Paper Vol. 10 No. 2, 2024). Although Chile's privacy law, Law No. 19,628 of 1999, was enacted after Directive 95/46/EC, the Directive 95/46/EC played no discernible role in its legislative deliberations. Instead, the law reflects a direct regulatory lineage from Spain's Organic Law 5/1992 on the automated processing of personal data. On this matter, *see* Pablo Viollier, El Estado de la Protección de Datos Personales en Chile [The State of Personal Data Protection in Chile] 8 (2017) (Chile).

[84] Carrillo & Jackson, *supra* note 58, at 178.

[85] Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, ETS No. 108, (Jan. 28, 1981), https://rm.coe.int/1680078b37.

[86] *See* Parraguez Kobek & Caldera, *supra* note 83, at 114.

[87] *See* Christian Pauletto, *Options Towards a Global Standard for the Protection of Individuals with Regard to the Processing of Personal Data*, Comput. L. & Sec. Rev., Apr. 2021, at 1, 12.

Uruguay, and Argentina) have formally acceded to the Convention.[88] Accession reflects a commitment to internationally recognised principles, thereby embedding domestic legislation within a broader framework of human rights and privacy protection.

With the enactment of the G.D.P.R., another wave of data protection laws took place in the region.[89] Brazil and Ecuador exemplify this trend, with Brazil adopting the *Lei Geral de Proteção de Dados Pessoais* [hereinafter L.G.P.D.] in 2018 and Ecuador following in 2021.[90] In 2018, Uruguay amended its 2008 data protection law to integrate core G.D.P.R. elements.[91] Chile amended its 1999 data privacy law in 2024, also following the G.D.P.R. model.[92]

The influence exerted by the possibility of facilitating cross-border data flows with Europe cannot be disregarded as one of the reasons for following such a regulatory approach, either through accession to Convention 108 or recognition as a third country offering an adequate level of protection through a European Commission decision.[93] However, the reality is that only three countries in the region (Mexico, Argentina, and Uruguay) have acceded to Convention 108 (Argentina and Uruguay have signed Convention 108+), and two countries have an adequacy decision from the E.U. (Argentina, Decision 2003/490/EC; and Uruguay, Implementing Decision 2012/484/EU).

It is worth noting the creation in 2003 of the Ibero-American Data Protection Network [hereinafter R.I.P.D.], which has played a central role in advancing the European model of data privacy,[94] with Spain at the forefront of this process,[95] issuing standards and recommendations that Latin American countries could adopt. From the regulatory perspective, one of the main milestones in the work of the R.I.P.D. is the approval in June 2017, in the framework of the XVI Ibero-American Meeting in Santiago de Chile, of the Standards for Personal Data Protection for Ibero-American States,[96] which the European

[88] *See* Eduardo Bertoni, *Convention 108 and the GDPR: Trends and Perspectives in Latin America*, Comput. L. & Sec. Rev., Apr. 2021, at 1.

[89] *See* Carrillo & Jackson, *supra* note 58, at 178.

[90] *Id.* at 240.

[91] *Id.* at 205.

[92] Lucas MacClure et al., Una introducción a la nueva Ley sobre Protección de Datos Personales y su relevancia para el Derecho de la Libre Competencia [An Introduction to the New Law on Personal Data Protection and Its Relevance for Competition Law] 26 (2024) (Chile).

[93] Alexandre Veronese et al., *The Concept of Personal Data Protection Culture from European Union Documents: A "Brussels effect" in Latin America?*, 9 UNIO - EU L.J. 58, 78 (2023) (Belg.).

[94] *See* Carrillo & Jackson, *supra* note 58, at 196.

[95] *See* Elías Chavarría-Mora, *(Lack of) Patterns in Commitment: Data Protection in the Latin America and Caribbean Personal Data Protection Laws*, Soc. Media + Soc'y, Apr-June 2025, at 1, 2.

[96] Ibero-American Network on Data Protection, *Standards for Personal Data Protection for the Ibero-American States* (June 20, 2017), https://www.redipd.org/sites/default/files/2022-04/standars-for-personal-data.pdf.

Commission has supported.[97] These standards constitute a set of guidelines that may contribute to the issuance of regulatory initiatives for the protection of personal data in the Ibero-American region, which encompasses those countries that do not have these regulations yet, or, in the case where they may serve as a reference for the modernisation and updating of existing legislation. In this sense, the primary purpose of these standards is to establish common principles and rights for the protection of personal data, thereby establishing homogeneous rules across the Ibero-American region. The preamble to the Standards for Personal Data Protection for Ibero-American States cites Convention 108 and the G.D.P.R. as key international instruments influencing its development. It acknowledges the G.D.P.R. as a benchmark for crafting national data protection laws in Ibero-America.

This evolution shows more than a technical effort to harmonise data protection rules; it reflects the gradual embedding of European approaches within Latin American digital regulatory thought. Grounding privacy rights in common principles and aligning national laws with international benchmarks such as Convention 108 and the G.D.P.R. has established the basis for a broader culture of governance over information technologies. That orientation extends well beyond traditional data protection, reaching domains where personal data drives technological innovation, most prominently A.I. The parallels are striking. Both regimes govern cross-border markets, aim to balance innovation with the protection of individual rights, and confront persistent challenges of accountability, transparency, and fairness. In this light, the regulatory trajectory established through data protection does more than offer a template; it lays the groundwork for A.I. governance. It furnishes policymakers with conceptual tools and institutional practices that can be recalibrated for new technological contexts, ensuring that the principles of data governance continue to shape the design, deployment, and oversight of A.I. systems.

Building on this regulatory trajectory, it is possible to underscore the relevance of the E.U. A.I. framework for Latin America, particularly in contexts where A.I. systems intersect with personal data.[98] Data protection principles are not simply legal obligations. They form the foundation for robust data governance practices that support the design, development, and deployment of A.I. systems. Clear rules on data collection, processing, and usage help ensure that A.I. operations incorporate transparency, accountability, and controllable bias mitigation from the very beginning. In B2C environments, where personal data plays a central role in A.I. functionality, the

[97] Superintendencia de Industria y Comercio (SIC), *Colombia and the Ibero-American Data Protection Network (RIPD)* (July 24, 2025), https://sedeelectronica.sic.gov.co/international-relations/colombia-and-iberoamerican-data-protection-network-ripd.

[98] *See* Siegmann & Anderljung, *supra* note 19, at 70.

application of these rules provides both a conceptual and practical framework for regulating A.I., guiding policymakers and developers toward responsible and trustworthy systems.[99]

A factor that contributes to this influence is the phenomenon identified by Papakonstantinou and De Hert as "G.D.P.R. mimesis." This concept captures how new regulatory frameworks replicate the structure, principles, and institutional architecture of the G.D.P.R. The G.D.P.R. has become a cornerstone of data protection law, yet its overwhelming influence has constrained legislators' creativity in regulating digital technologies. Its dominance is such that lawmakers often feel compelled to adopt its protective approach when introducing ambitious regulatory frameworks with broad societal impact.[100]

Viewed through this lens, A.I. legislation in Latin America is emerging within a data protection-infused framework, as the rules governing personal data do not merely coexist with A.I. regulations but actively shape them. Following the G.D.P.R.-inspired logic of mimesis allows policymakers to ensure that A.I. governance is not only legally coherent but also practically enforceable, supporting the responsible development and use of A.I. technologies. In this sense, the E.U. model could function as both a template and a touchstone, demonstrating how data protection principles can provide the foundation for the complex regulatory architecture necessary for effective A.I. oversight.

3. TRACING THE RECEPTION OF THE EUROPEAN A.I. REGULATORY APPROACH IN LATIN AMERICA THROUGH DATA PROTECTION PROVISIONS

Some of the first regulatory efforts to address data-driven A.I. systems in Latin America have been closely linked to the evolution of data protection law. Because A.I. systems often process personal data, existing data protection provisions provide both a conceptual and practical foundation for regulating these technologies. Examining these A.I.-related data protection rules is therefore essential, as they have already been incorporated into the legal frameworks of certain Latin American countries, serving as a point of entry into European-inspired approaches to A.I. governance. Understanding this intersection helps clarify why data protection norms continue to shape the emerging regulatory landscape for A.I. in the region.

[99] *See* Pablo Trigo Kramcsák, *Can Legitimate Interest Be an Appropriate Lawful Basis for Processing Artificial Intelligence Training Datasets?*, Comput. L. & Sec. Rev., Apr. 2023, at 1 (U.K.).

[100] *See* Papakonstantinou & de Hert, *supra* note 18, at 1.

Through their next-generation data protection laws that follow the G.D.P.R. model, some Latin American countries are undertaking the first regulatory attempts to address specific challenges related to the use of A.I. systems, as we will explore further in the following section. Indeed, the G.D.P.R. and its enforcement by D.P.A.s[101] play a relevant role in mitigating some A.I. effects, particularly when these systems involve processing personal data. A.I. has been intertwined with the development of data protection law from its inception, whose adaptive nature ensures its continued relevance in addressing contemporary A.I.-related issues.[102] As a consequence, A.I. is addressed within the scope of the G.D.P.R., aligning with its existing conceptual framework.[103]

The G.D.P.R. provides rules for big data processing, profiling, and automated decision-making systems. Among other aspects, the G.D.P.R. grants individuals (in Article 22) the right to know when automated decision-making, including profiling, is being used to make decisions that have legal or similarly significant effects on them.[104] It also grants them the right to obtain meaningful information about the logic involved and the consequences of such processing. Individuals also have the right to object to such processing and request human intervention.

Drawing on these foundations, some Latin American countries are translating G.D.P.R. standards into domestic frameworks, adapting them to local contexts while preserving core protections. The G.D.P.R.'s rules on automated decision-making, profiling, and data subject rights provide a conceptual blueprint for regulating A.I. systems that process personal data. These provisions demonstrate how data protection law functions as the initial point of regulatory engagement with A.I., providing concrete safeguards against algorithmic harms. Examining national implementations, such as those in Brazil, illustrates how these A.I.-related norms are operationalised, reflecting both alignment with European rules and adaptations to local legal and social priorities.

[101] *See* Gabriela Zanfir-Fortuna, *How Data Protection Authorities Are De Facto Regulating Generative AI*, Future Of Privacy Forum Blog (Sept. 12, 2023), https://fpf.org/blog/how-data-protection-authorities-are-de-facto-regulating-generative-ai/.

[102] *See* Gabriela Zanfir-Fortuna, *Why data protection legislation offers a powerful tool for regulating AI*, LSE: EUROPP Blog (Febr. 10, 2025), https://blogs.lse.ac.uk/europpblog/2025/02/10/why-data-protection-legislation-offers-a-powerful-tool-for-regulating-ai/(U.K.).

[103] *See* Sartor & Lagioia, *supra* note 72.

[104] Article 22 of the GDPR builds on Article 15 of the Data Protection Directive, which focused on decisions made solely by automated means. On this matter, *see* Olivia Tambou, *Art. 22: Automated Individual Decision-making, Including Profiling*, General Data Protection Regulation: Article-by-Article Commentary 525 (Indra Spiecker gen. Döhmann et al. eds., 2023) (Ger.).

Brazil's General Data Protection Law[105] stipulates in Article 20 that data subjects have the right to request the review of decisions made solely automated processing of personal data affecting their interests, including decisions intended to define their personal, professional, consumer, and credit profiles, or aspects of their personality. Additionally, if requested, the controller shall provide clear and adequate information on the criteria and procedures used for automated decision-making, subject to commercial and industrial secrecy. Finally, the national authority may audit to verify discriminatory aspects in the automated processing of personal data.[106]

Following years of legislative deliberation in Chile, the 1999 Personal Data Protection Law (Law No. 19.628, Law on Protection of Private Life) was comprehensively updated with the enactment of Law No. 21.719, published in the Official Gazette in December 2024.[107] This new legislation marks a substantial reform of the national data protection framework, bringing it closer to international standards and addressing emerging challenges in digital governance. The principles and substantive rules of the G.D.P.R. have strongly influenced the amendment process. In this vein, the new Personal Data Protection Law establishes in Article 8 bis that data subjects have the right to object to and not be subject to decisions based on automated processing of their data, including profiling, that produces legal effects or significantly affects them, except when the decision is necessary for the conclusion or performance of a contract between the data subject and the controller; when data subjects give their consent; or when provided by law (under certain safeguards). In any case, the controller must adopt the necessary measures to ensure the rights and freedoms of data subjects, their right to information and transparency, the right to obtain an explanation, the right to human intervention, the right to express their point of view, and the right to request a review of the decision.

Given the preceding, Brazil and Chile, having enacted next-generation data protection laws inspired by the GDPR, are beginning to incorporate regulatory measures

[105] *See* https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. For unofficial English translation, *see* https://cyberbrics.info/wp-content/uploads/2020/02/The-Brazilian-LGPD-English-Version.pdf, translated Luca Belli, Laila Lorenzon and Luã Fergus. (Braz.).

[106] Brazil's data protection authority (ANPD) published Technical Note No. 12/2025 on 15 May 2025 summarising public input in relation to the establishment of interpretative parameters for the application of Article 20 LGPD, https://www.gov.br/anpd/pt-br/acesso-a-informacao/participacao-social/outras-acoes/documentos/ts-06-2024-nt-12-2025-consolidacao-das-contribuicoes.pdf/view (accessed Aug. 19, 2025) (Braz.).

[107] Ley Núm. 21.719: Regula la Protección y el Tratamiento de los Datos Personales y Crea la Agencia de Protección de Datos Personales, https://www.bcn.cl/leychile/navegar?idNorma=1209272 (accessed Sept. 12, 2025) (Chile).

that address specific uses and effects of A.I. systems.[108] Although this first regulatory attempt is sectoral and not comprehensive, it cannot be ignored that it is framed within the European vision for regulating digital technologies and presents an approach that seeks to harmonise its various regulations. It should be noted that the provisions of the A.I. Act on the processing of personal data do not overlap with the rules of the G.D.P.R. "The A.I. Act and the G.D.P.R. are bound to work in tandem – they are both grounded on Article 16 T.F.E.U. and they have many areas where they complement each other, as well as areas where they could be better coordinated so that both their goals are achieved".[109] This scenario, in some way, could contribute to framing the regional discussion around comprehensive A.I. laws using the European framework as a model.

In this evolving regulatory landscape, a closer examination of G.D.P.R. mimesis reveals how data protection logic shapes A.I. regulation. Its influence spans high-level principles, legislative structure, and oversight mechanism design. Definitional mimesis appears in the use of familiar G.D.P.R. terminology and the introduction of new actors who create a regulatory system reminiscent of the G.D.P.R. Substantive mimesis is evident in provisions such as the principle of accountability, which clearly reflects G.D.P.R. influence. Institutional mimesis emerges through the establishment of cooperation mechanisms, coordination procedures, and risk assessment requirements, alongside supervisory authorities at the Member State level. Together, these dimensions illustrate how G.D.P.R.-inspired logic informs A.I. governance, fostering transparency, accountability, and bias mitigation across A.I. systems.[110]

It is worth noting that the R.I.P.D. published the "General Recommendations for Data Processing in Artificial Intelligence" in 2019.[111] These recommendations are aimed at developers of A.I. systems, guiding them from the design phases to ensure compliance

[108] It is also worth noting that Ecuador's Organic Law on the Protection of Personal Data, enacted in 2021, establishes in Article 20 the right not to be subject to a decision based solely or partially on automated processing, following a formulation similar to that of Article 22 of the GDPR. *Cf. See* Ecuador, Ley Orgánica de Protección de Datos Personales (May 26, 2021), https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf (accessed Aug. 19, 2025) (Ecuador) Uruguay's data protection law, Ley 18.331 (2008), explicitly grants individuals the right to object to decisions based solely on automated processing (Art. 16). The same provision ensures access to information about the logic and criteria underlying such AI-driven decisions. On this matter, *see* Alexandre Veronese & Amanda Nunes Lopes Espiñeira Lemos, *Regulatory Paths for Artificial Intelligence in Latin American Countries with Data Protection Law Frameworks: Limits and Possibilities of Integrating Policies*, Revista Latinoamericana de Economía y Sociedad Digital, Aug. 2021, at 1, 13 (Arg.).

[109] *See* Gabriela Zanfir-Fortuna, *GDPR and the AI Act Interplay: Lessons from FPF's ADM Case Law Report*, Future of Privacy Forum (Feb. 27, 2024), https://fpf.org/blog/gdpr-and-the-ai-act-interplay-lessons-from-fpfs-adm-case-law-report/.

[110] *See* Papakonstantinou & de Hert, *supra note* 18, at 48-49.

[111] *See General Recommendations for the Processing of Personal Data in Artificial Intelligence*, Red Iberoamericana de Proteccion de Datos, https://www.redipd.org/en/documents/guide-general-recommendations-processing-personal-data-ai.

with personal data protection regulations. This approach was reflected in May 2023, when the R.I.P.D. authorities initiated a coordinated supervisory action concerning the ChatGPT service, focusing on its data processing activities.[112]

4. EMERGING REGULATORY A.I. TRENDS IN LATIN AMERICA

While the A.I. Act's regulatory structure has close alignment with the E.U.-specific institutional structures, posing significant barriers to its transposition beyond the Union's jurisdiction,[113] since its entry into force on the first of August 2024, the A.I. Act has resonated in Latin America, prompting these countries to discuss the necessity of regulating the use of artificial intelligence and how to do so effectively.

4.1. NATIONAL PLANS AND STRATEGIES

From the outset, it is evident that the Latin American region has been actively formulating national A.I. strategies to govern the adoption and management of A.I. technologies. The following analysis will examine the region's initiatives chronologically.[114]

Mexico was one of the first Latin American countries to raise awareness of the need to develop an artificial intelligence national strategy, launching a report in March 2018.[115] Yet the change in the presidential administration in 2018 led to a pause in the plan's development. In the following year, Argentina, Uruguay, and Colombia launched national A.I. strategies. The Argentinian National Plan for 2019-2029, which started to be crafted in 2018, primarily focuses on enhancing state productivity,[116] while both

[112] *See Las autoridades de la Red Iberoamericana de Protección de Datos Personales inician una acción coordinada en relación con el servicio ChatGPT*, Red Iiberoamericana de Proteccion de Datos (May 8, 2023) https://www.redipd.org/noticias/autoridades-red-iberoamericana-de-proteccion-de-datos-personales-inician-accion-chatgpt. To date, there has been no other official initiative that could assess the impact of these Recommendations.

[113] *See* Greenleaf, *supra* note 30, at 4.

[114] This section examines initiatives across Latin American countries, excluding the Caribbean.

[115] *See* Emma Martinho-Truswell et al., Towards an AI Strategy in Mexico: Harnessing the AI Revolution (2018) (U.K.).

[116] *See* Presidencia de la Nación, *Plan Nacional de Inteligencia Artificial*, https://oecd-opsi.org/wp-content/uploads/2021/02/Argentina-National-AI-Strategy.pdf (Arg.).

Uruguay's[117] and Colombia's[118] plans, launched in the same year, prioritise the transformation of the public sector through A.I. initiatives.

In 2021, Brazil introduced its A.I. Strategy, emphasising ethical principles, governance frameworks, and innovation brought by A.I.[119] In the same year, Chile also published its plan, integrating the tenets of human rights and sustainable development.[120] Conversely, Peru's 2021-2026 strategy aspires to situate the country as a leader in regional A.I. advancements[121] while Panama is currently engaged in discussions regarding its own A.I. strategy.

In October 2024, the High-Level Authorities Summit on A.I. Ethics held in South America and the Caribbean culminated in the Declaration of Montevideo, which reaffirms a commitment to upholding human rights, democracy, and the sustainable development of A.I. technologies.[122] The summit also led to the approval of a regional A.I. Roadmap delineating five priority areas: governance and regulation, talent development, the protection of vulnerable groups, environmental sustainability, and infrastructure enhancement. It is noteworthy, however, that not all South American nations were represented at the summit, with official delegations from selected countries, including Brazil, Chile, Colombia, and Peru.

4.2. LEGISLATIVE ACTIONS

While Latin American countries have been active in publishing national strategies, they have yet to approve comprehensive bills to regulate A.I., though various proposals have emerged.

[117] *See* Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (Agesic), *Estrategia de Inteligencia Artificial para el Gobierno Digital* (2020), https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/estrategia-inteligencia-artificial-para-gobierno-digital/estrategia (Uru.).

[118] *See* Ministerio de Ciencia, Tecnología e Innovación, *Hoja de Ruta para la Adopción Ética y Sostenible de la Inteligencia Artificial en Colombia* (2024), Hoja de Ruta AI (PDF) (Colom.).

[119] *See Estratégia Brasileira de Inteligência Artificial (EBIA)* (2021), https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/estrategia-brasileira-de-inteligencia-artificial (Braz.).

[120] *See* Ministerio de Ciencia, Tecnología, Conocimiento e Innovación, *Política Nacional de Inteligencia Artificial* (2021), https://minciencia.gob.cl/uploads/filer_public/bc/38/bc389daf-4514-4306-867c-760ae7686e2c/documento_politica_ia_digital_.pdf (Chile).

[121] *See* Sergio Vélez Maldonado, *Estrategia Nacional de Inteligencia Artificial en Perú: Un Análisis Exhaustivo*, FuturIA (July 7, 2024), https://futuria.substack.com/p/estrategia-nacional-de-inteligencia-31e.

[122] *See* Declaration Of Montevideo (2024), https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/sites/agencia-gobierno-electronico-sociedad-informacion-conocimiento/files/documentos/noticias/EN%20-%20Montevideo%20Declaration%20approved.pdf [https://parlamentomercosur.org/innovaportal/file/12593/1/parlandino.pdf].

The first identified legal initiative to regulate A.I. in the region was taken by Peru. In July 2023, Law No. 31814 was approved, aiming to promote the use of A.I. in favour of the economic and social development of the country.[123] Yet, three other proposals regarding A.I. are currently pending. None of them aims to comprehensively regulate the technology, as the EU's A.I. Act does. Bill of Law No. 07651/2023-CR, introduced in April 2024, proposes to regulate the use of algorithms and AI systems for real-time vehicle recognition and for tampered license plates. The second proposal, No. 2338/2023: 05182/2022, seeks to promote the use of A.I. in Peru's ground transportation system, which has been discussed since its introduction in May 2023. The third proposal, No. 07033/2023, aims to establish a general framework to regulate A.I. in the country, adopting a risk-based approach similar to the A.I. Act.[124] It designates the task of supervising A.I. systems to the Government Agency of Digital Transformation (*Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros*), which will inspect, investigate. Audit A.I. systems, create a public registry, receive complaints, and prohibit the deployment of A.I. systems that violate the proposed law.

Argentina has followed a similar path. The country has not passed any regulations on the topic, but various proposals have been introduced ,demonstrating varying levels of influence from the EU's A.I. Act. On June 4, 2023, Morales Gorleri, a member of the opposition party, introduced PL 2504/2023 to the House of Representatives, a comprehensive framework for A.I. regulation aimed at establishing measures to promote the ethical development of A.I., protect human rights, ensure transparency and accountability, and foster innovation. On the eighth of August 2023, Pamela Calletti (member of the party at the government) introduced PL 3161/2023 to the House of Representatives. This alternative bill establishes a governmental body to oversee and advise on A.I. policy, composed of public officials to promote A.I. research, ethics, and public awareness. Finally, on the fourteenth of August 2023, Senator Juan Carlos Romero, member of the Justicialist Party, introduced PL 1743/2023 to the Senate. Compared with other regulations, Romero's proposal most closely resembles the EU's A.I. Act. It aims to establish controls and guiding principles for the development, implementation, and use of A.I. systems to protect human dignity, human rights, and the well-being of people by defining different risk levels for A.I. systems, including "limited risk," "minimal or no risk," "high risk," and "unacceptable" systems.[125]

[123] *See* Congreso de la República del Perú, *Ley N.º 31814, Ley que promueve el uso de la inteligencia artificial en favor del desarrollo económico y social del país* [Law No. 31814, Law Promoting the Use of Artificial Intelligence for the Economic and Social Development of the Country] (July 5, 2023) (Peru).

[124] *See* Proyecto de Ley nº 07033/2023-CR (2023) (Peru).

[125] *See* EGA, Artificial Intelligence: Latin America's Regulatory and Policy Environment (2024).

Also in August 2023, Uruguay submitted a short A.I. Regulation Proposal No. 1737/2023. Yet the proposal is quite limited and only emphasises that the deployers of A.I. systems must label their systems. However, the proposal does not include any labelling system or any form of authority to regulate A.I. systems.[126] Additionally, Uruguay's National AI Strategy 2024-2030 was approved on the twenty-first of November 2024 by the Public Sector Strategic Committee for Artificial Intelligence and Data.[127] Unlike the original 2019 strategy, which focused primarily on the public sector (titled "Artificial Intelligence for Digital Government"), the new 2024-2030 strategy covers both public and private sectors.

In the following month, the first proposal to regulate A.I. was submitted to the Colombian House of Representatives. The bill, PL 200/2023, was a statutory law focused on labor rights in the context of A.I., aiming to address the potential for job displacement arising from the implementation of A.I. systems in companies. Following the bill's rejection, three other proposals emerged in the Senate. PL 059/2023 established public policy guidelines for the development, use, and implementation of A.I., focusing on creating a framework for data protection, intellectual property protection, and a code of ethics for A.I. use. PL 091/2023, which aims to mandate a duty of information for the responsible use of A.I., ensuring transparency, ethical practices, and the protection of user rights. PL 130/2023 returns to the topic of A.I. and labour rights, aiming to protect workers' rights and ensure the proper use of A.I., guaranteeing job stability and harmonising technological advancements with labour laws. Finally, Proposal 154/2024 is a more comprehensive proposal focusing on general A.I. regulation across all sectors by introducing a risk-based approach, classifying A.I. systems as "unacceptable," "high risk," "limited risk," and "minimal risk," similar to the EU A.I. Act. In August 2024, the Executive Government established a Commission to enhance debates and dialogue on the regulation of A.I. The Commission is tasked with unifying the submitted projects and constructing public policies regarding A.I. while respecting principles of transparency, equality, and justice.[128] When it comes to the establishment of A.I. enforcement authorities, among the four projects currently running in Colombia, PL 059/2023, PL

[126] *See* Proyecto de ley con exposición de motivos presentado por el señor Senador Juan Sartori (2023) (Uru.).

[127] *See* Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento, *Se aprobó la Estrategia Nacional de Inteligencia Artificial 2024 - 2030* [The National Artificial Intelligence Strategy 2024 – 2030 Was Approved] (Nov. 22, 2024), https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/noticias/se-aprobo-estrategia-nacional-inteligencia-artificial-2024-2030 (Uru.).

[128] *See* Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), *Colombia avanza en la regulación de la inteligencia artificial con la creación de Comisión Accidental en el Congreso para articular proyectos en curso* [Colombia advances in the regulation of artificial intelligence with the creation of an Accidental Commission in Congress to coordinate ongoing projects] (Aug. 27, 2024) (Colom.).

091/2023, PL 130/2023, and PL 154/2024, only the last mentions possible regulatory agencies, yet it does not designate any.

In June 2024, Ecuador proposed a bill to regulate A.I., titled "*Proyecto de Ley Orgánica de Regulación y Promoción de la Inteligencia Artificial en Ecuador*".[129] The bill is a comprehensive proposal that mirrors the E.U.'s A.I. Act by adopting a risk-based approach, classifying AI systems into different categories to apply a proportionate level of regulation. The proposal is still under consideration at the National Assembly. It has included a dedicated chapter establishing an A.I. Authority, named *Autoridad Nacional de Regulación de Inteligencia Artificial*, which will be responsible for implementing and enforcing A.I. regulations in Ecuador, ensuring compliance with this law.

The following table summarises all the proposals in chronological order.

Country	**Year / Date**	**Initiative**	**Status**
Peru	2022	Bill No. 2338/2023: 05182/2022 – AI use in ground transportation; under discussion	Proposal
	July 2023	Law No. 31814 – Promotes AI for economic and social development	Approved
	April 2024	Bill No. 07651/2023-CR – Regulates AI for real-time recognition of stolen/tampered vehicles	Proposal
	2024	Bill No. 07033/2023 – General AI framework (risk-based, AI Act-inspired); supervisory role given to the Government Agency of Digital Transformation	Proposal
Argentina	June 4, 2023	PL 2504/2023 – Ethical AI development, human rights protection, transparency, accountability, and innovation	Proposal
	Aug 8, 2023	PL 3161/2023 – Establishes a governmental AI advisory and oversight body	Proposal
	Aug 14, 2023	PL 1743/2023 – Risk-based AI controls to protect human dignity and rights	Proposal
Uruguay	Aug 2023	Proposal No. 1737/2023 – Requires labeling of AI systems; no supervisory authority	Proposal
Colombia	Sept 2023	PL 200/2023 – Defines and regulates AI aligned with human rights standards	Rejected
	Late 2023	PL 059/2023 – Public policy guidelines for AI development and use	Proposal
	Late 2023	PL 091/2023 – Duty to inform; transparency and user rights	Proposal
	Late 2023	PL 130/2023 – AI and labor law harmonization	Proposal
	2024	PL 154/2024 – Comprehensive AI framework inspired by EU AI Act	Proposal
Ecuador	June 2024	Proyecto de Ley Orgánica de Regulación y Promoción de la IA – Creates National AI Regulatory Authority	Proposal

Table 1: Overview of AI-related legislative proposals in selected Latin American countries

[129] *See* Proyecto de Ley Orgánica de Regulación y Promoción de la Inteligencia Artificial en Ecuador (As. Patricia Núñez / 450889), https://www.asambleanacional.gob.ec/es/multimedios-legislativos/97303-proyecto-de-ley-organica-de-regulacion (Ecuad.).

Overall, it is possible to observe that, while initially there was a surge of regulatory proposals to regulate AI systems in Latin American countries, most likely inspired by the EU's AI Act, this impulse has not, so far, resulted in any comprehensive regulation similar to the EU's. This might be due to multiple factors. As previously mentioned, the EU's AI Act has close alignment with the EU-specific institutional structures, demanding that Latin American countries adapt this regulatory model to their social and cultural concerns.[130] Moreover, most Latin American countries are considered emerging markets that actively embrace AI technologies, with the expectation of increasing economic growth and technological development.[131] This desire may hinder the approval of comprehensive regulations that may represent the halting of AI innovation.[132]

5. EXPLORING THE BRAZILIAN AND CHILEAN A.I. GOVERNANCE SCHEMES

This section focuses on the emerging AI governance frameworks in Brazil and Chile. The decision to focus on these two countries reflects a combination of legal, economic, political, and regional factors that render their regulatory trajectories particularly relevant when considered alongside the European Union's approach.

Brazil and Chile, both civil law jurisdictions, offer distinct yet potentially complementary perspectives on AI governance in Latin America. As a key regional actor and member of both BRICS and MERCOSUR, Brazil holds a prominent position in shaping regulatory developments across the region.[133] Its proposed AI framework reflects domestic priorities and broader geopolitical considerations, with possible implications for neighbouring countries within these regional blocs.[134] Chile, by contrast, is characterised by an open economy and an extensive network of free trade and digital trade agreements. Its strong ties to the Asia-Pacific region have positioned it as an early

[130] *See* María L. Flórez Rojas, *The Shaping of AI Policies in Latin America: A Study of International Influence and Local Realities*, *in* PUBLIC GOVERNANCE AND EMERGING TECHNOLOGIES: VALUES, TRUST, AND REGULATORY COMPLIANCE 263 (Jurgen Goossens et al. eds., 2025).

[131] *See* Anastassia Lauterbach, *Artificial Intelligence and Policy: Quo Vadis?*, 21 DIGIT. POL'Y, REGUL. & GOVERNANCE 238 (2019) (U.K.).

[132] *See* Meera Sarma et al., *Challenges and Opportunities of Ethical AI and Digital Technology Use in Emerging Economies*, *in* ELGAR COMPANION TO REGULATING AI AND BIG DATA IN EMERGING ECONOMIES 42 (Mark Findlay et al. eds., 2023).

[133] *See* Kramcsak, *supra* note 83, at 4.

[134] *See Brazil Places AI Governance at Top of BRICS and G20 Negotiation Agenda*, TV BRICKS (Feb. 11, 2025), https://tvbrics.com/en/news/brazil-places-ai-governance-at-top-of-brics-and-g20-negotiation-agenda/.

mover in digital regulation,[135] and a "regional leader in promoting AI regulations",[136] seeking alignment between domestic governance and international standards.

The experiences of Brazil and Chile provide a valuable comparative perspective for understanding how Latin American countries engage with global regulatory debates while responding to their specific institutional and socio-economic contexts. Although both are adapting their legal systems to address the challenges posed by A.I., they do so within different institutional configurations. In addition, both countries have taken active steps in adopting and regulating A.I., making them particularly relevant case studies in the Latin American context.[137] Their approaches highlight the practical and normative considerations of balancing innovation with legal safeguards.

Comparing these developments with the European Union's supranational regulatory model also offers a broader understanding of the potential trajectories of A.I. governance in Latin America. While the E.U. has advanced a comprehensive legal framework, Brazil and Chile are progressing at different speeds, influenced by political priorities, economic conditions, and institutional readiness.

5.1. BRAZILIAN AI GOVERNANCE MODEL

5.1.2. BACKGROUND

The European A.I. Act commenced its Brussels Effect in Brazil even before it was approved. Brazilian legislators' first tentative attempt to regulate A.I. began with Proposal No. 5.051/2019,[138] closely followed by Proposal No. 21/2020 initiated by the Chamber of Deputies in 2020.[139] This proposal was considered a succinct 10-Article "anti-regulation regulation" since it only enacted recommendations with no

[135] *See* Pablo Trigo Kramcsák & Michelle Bordachar Benoit, The (Potential) Impact of the Digital Economy Partnership Agreement on the Future of Cross-Border Personal Data Flows (2023).

[136] Andrés Mosqueira & Shaanty E. Rubio Gonzalez, *Foster Innovation or Mitigate Risk? AI Regulation in Latin America*, White & Case (Nov. 18, 2024), https://www.whitecase.com/insight-our-thinking/latin-america-focus-2024-ai-regulation.

[137] *See* Airlie Hilliard, *How Is Brazil Leading South America's AI Legislation Efforts?*, Holistic AI (Nov. 20, 2023), https://www.holisticai.com/blog/brazil-ai-legislation-proposals.

[138] *See* Senado Federal (Brazil), *Projeto de Lei No. 5.051, de 2019* [Bill No. 5.051 of 2019], (Braz.), https://www25.senado.leg.br/web/atividade/materias/-/materia/138790.

[139] *See* Câmara dos Deputados (Braz.), Projeto de Lei No. 21, de 2020 [Bill No. 21 of 2020], (Braz.), https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2236340&fichaAmigavel=nao.

enforcement schemes and no creation of new rights related to the ones impacted by A.I. systems, only referring to existing rights in the Brazilian legal framework.[140]

However, this first proposal was criticised for its swift approval process in the Chamber of Deputies, with no public participation, and for its reduced regulatory framework, which did not regulate or enact any new rights concerning A.I. risks. As a response, a Commission of 18 Jurists ("CJSUBIA") was formed, and after nine months of work, the Commission proposed a replacement ("*substitutivo*") Proposal to the Senate.

In 2023, proposal 2338/2023 (now in the Senate) was submitted, inspired by the Commission of Jurists' draft and the previous Chamber of Deputies. This new proposal is considered to be aligned with the already approved European A.I. Act, although with some differences,[141] such as the development of three main pillars: the creation of rights for those affected by A.I. systems, a risk-based approach (similar to the European A.I. Act), and the establishment of governance measures applied to companies that develop or deploy A.I. systems.[142]

5.1.3. THE GOVERNANCE FRAMEWORK

As mentioned, the most recent Brazilian proposal is grounded in the European A.I. Act but has a few caveats, including the governance framework. The structure of governance brought by the proposal establishes on Article 40, the National System of Regulation and Governance of Artificial Intelligence ("*Sistema Nacional de Regulação e Governança de Inteligência Artificial* – S.I.A.") [hereinafter S.I.A.], which is a multifold system which is formed by multiple regulation authorities namely: the general coordinating authority responsible for regulating artificial intelligence which according to the new amendments to the proposal will be the Brazilian Data Protection Authority [hereinafter

[140] *See* Laura Schertel Mendes, *Projeto de Lei da Inteligência Artificial: armadilhas à vista* [Artificial Intelligence Bill: Pitfalls Ahead], O Globo (Nov. 26, 2021), https://blogs.oglobo.globo.com/fumus-boni-iuris/post/laura-schertel-mendes-pl-da-inteligencia-artificial-armadilhas-vista.html.

[141] *See* Carolina Aguerre, *Strategies, Norms, Cooperation: Three Approaches to AI Governance in Latin America*, KU Leuven: AI Summer School Blog (Oct. 15, 2024), https://www.law.kuleuven.be/ai-summer-school/blogpost/Blogposts/strategies-norms-cooperation-three-approaches-to-ai-governance-in-latin-america.

[142] *See* Laura Schertel Mendes, *A regulação da inteligência artificial no Brasil: Fundamentos do anteprojeto de lei apresentado pela Comissão de Juristas do Senado Federal* [*The Regulation of Artificial Intelligence in Brazil: Fundamentals of the Draft Bill Presented by the Senate Federal Commission of Jurists*], Fumus Boni Iuris (Jan. 27, 2023), https://oglobo.globo.com/blogs/fumus-boni-iuris/post/2023/01/laura-schertel-mendes-a-regulacao-da-inteligencia-artificial-no-brasil.ghtml; *see also* Augusto Castro, *IA: relator apresenta proposta alinhada com regulamentos da Europa e dos EUA* [AI: Rapporteur Presents Proposal Aligned with European and U.S. Regulations], Senado (Apr. 24, 2024), (Braz.), https://www12.senado.leg.br/noticias/materias/2024/04/24/ia-relator-apresenta-proposta-alinhada-com-regulamentos-da-europa-e-dos-eua.

A.N.P.D], State's A.I. regulators, the Administrative Council of Defense and Competition, self-regulatory entities, and certification entities.

The main objective of this System is to enhance and harmonise the regulatory competencies of its multiple regulatory authorities with the system's general coordinator authority and with other agencies that are not part of S.I.A., such as environmental agencies and consumer protection (Art. 40 § 2).

Amongst the competencies of the S.I.A's general coordinator authority is to be the Brazilian international representative when it comes to matters related to A.I. (Art. 41, I), to elaborate in coordination with the other agencies that part of the System binding decisions related to the following matters: the exercise of the A.I. rights, shape and form of public information shared regarding the use of A.I. systems, proceedings, and requisites for the certification of the development of high-risk A.I. systems, proceedings and requisites of algorithmic impact assessments, and proceedings for communicating grave incidents, especially when fundamental rights are impacted (Art. 41, II). Moreover, the S.I.A.'s general coordinator authority has the competence to elaborate non-binding opinions about the development, implementation, and use of A.I. systems, celebrate regulatory agreements with the other S.I.A.'s authorities, express non-binding opinions in every legislative regulation regarding these regulatory authorities, exercise legislative, regulatory and sanctioning powers when it comes to the use, development, and implementation of A.I. systems when there is no sectorial regulatory entity. Finally, the authority will be certified and will be able to give opinions on regulatory sandboxes (Art. 41 III to VII).

Article 43 of the Proposal describes the exclusive attributions and powers of the S.I.A.'s general coordinator authority, namely to protect the rights of those affected by A.I. systems, stimulate good practices, including the development of codes of conduct to the development and use of A.I. systems, cooperate with international authorities that regulate A.I., request information from A.I. systems deployed and developed by public authorities regarding the scope, data, and details of its development with the possibility of enacting opinions to guarantee the compliance to the law, celebrate regulatory agreements to eliminate non-compliance with the law, law uncertainties, and administrative processes, receive noncompliance complaints of other S.I.A. authorities, write annual reports, lead audits of A.I. systems, issue credentials to private audits companies and research institutions, receive anonymous complaints regarding A.I. systems, and develop rules and schemes to the development and use of responsible A.I. systems (Art. 43, I-XIII).

Yet, it is important to emphasise that the creation of an independent regulatory entity to regulate A.I. has been criticised by the Brazilian National Data Protection Authority [hereinafter, A.N.P.D.], which considers that there is significant overlap in competencies between the two agencies. For this reason, recent amendments have placed the A.N.P.D. as the leading authority responsible for regulating artificial intelligence in the S.I.A. system.[143]

Nevertheless, the A.N.P.D., as the leading authority responsible for coordinating the S.I.A. system, may address some concerns, but agency concerns may arise. When the L.G.P.D. was proposed in 2012 (an evident influence of the G.D.P.R.'s Brussels Effect), one of the biggest discussions was the Federal government's competence to regulate the protection of the fundamental right to data protection. As a result of this discussion, Constitutional Amendment No. 115/2022 added incise LXXIX to Article 5 of the Brazilian Constitution, granting the Brazilian government the authority to protect the right to personal data. Additionally, the amendment said Incise XXVI to Article 21, giving the Union the competence to "organise and visualise the protection and the treatment of personal data, under the legal terms" and Incise XXX to Article 22, giving the Union the competence "to legislate about data protection and the treatment of personal data". This resolved the unconstitutionality of the A.N.P.D.'s existence, although the L.G.P.D. was published before the constitutional amendment, which raises constitutional problems under Brazilian law. In this light, the same discussion may arise regarding the A.N.P.D.'s competence to regulate and oversee the enforcement of the Brazilian A.I. Act. Another constitutional amendment may be necessary to address this incompatibility, creating yet another constitutional conundrum.[144]

Besides the constitutional discussion, the efficiency of such a fragmented enforcement frame has also yet to be tested; however, the horizon does not look bright, drawing on examples from the G.D.P.R. Member States' enforcement practices.

[143] *See* the Legal Opinion of Deputy Eduardo Gomes (Braz.), https://legis.senado.leg.br/sdleg-getter/documento?dm=9640105&ts=1718733815121&rendition_principal=S; *see also* Ministério da Justiça e Segurança Pública, ANPD é formalizada como coordenadora do Sistema Nacional de Inteligência Artificial [ANPD Is Formalized as Coordinator of the National Artificial Intelligence System], Gov.br (June 20, 2024) (Braz.), https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-e-formalizada-como-coordenadora-do-sistema-nacional-de-inteligencia-artificial.

[144] There little to no scholarly sources on the topic. Most of the public debate took place in opinion pieces in relevant Brazilian media. *See* Felipe de Paula & Vitor Rabelo Naegele, *Há vício de iniciativa na criação da Autoridade Nacional de Proteção de Dados?*, [*Is There a Defect of Initiative in the Creation of the National Data Protection Authority?*], JOTA (July 26, 2018), https://www.levysalomao.com.br/files/publicacao/anexo/20180727165904_ha-vicio-de-iniciativa-na-criacao-da-autoridade-nacional-de-protecao-de-dados.pdf; *see also* Luis H. de Menezes Acioly et al., *A Emenda Constitucional nº 115 de 10 de fevereiro de 2022 e o enforcement da proteção de dados pessoais no Brasil* [*Constitutional Amendment No. 115 of 10 February 2022 and the Enforcement of Personal Data Protection in Brazil*], Revista de Investigações Constitucionais [J. Const. Rsch.], Oct. 2024, at 1 (Braz.).

Conflicting decisions, significant overlaps, high bureaucratic burdens, and legal uncertainty might pose obstacles for the Brazilian A.I. regulatory framework in the future. It should be noted that Belli et al. stress that Brazil's proposed A.I. Regulatory Framework "contradicts several existing legal provisions, notably regarding consumer protection, L.G.P.D. transparency and non-discrimination clauses".[145]

In this complex institutional landscape, Brazil's decision to position the A.N.P.D. as the general coordinating authority within the S.I.A. framework reveals both a pragmatic move to leverage existing regulatory expertise and a potential flashpoint for future constitutional and operational frictions. While this approach may help consolidate oversight and mitigate institutional fragmentation, it raises critical concerns regarding the legal soundness of the A.N.P.D.'s expanded mandate, given its original constitutional basis. Moreover, the coexistence of multiple sectoral regulators, certification bodies, and self-regulatory entities introduces layers of coordination that risk diluting accountability and undermining enforcement coherence. These challenges have already surfaced in jurisdictions implementing the G.D.P.R. Brazil's A.I. governance model, which thus reflects a balancing act between aligning with global normative trends and responding to domestic legal and institutional particularities.

5.2. CHILEAN A.I. GOVERNANCE MODEL

5.2.1. BACKGROUND

On April 12, 2023, a bill (parliamentary motion) was introduced to the Chilean Chamber of Deputies to regulate artificial intelligence systems, robotics, and related technologies across various applications (Bill No. 15,869-19).[146] The bill's primary objective was to establish a comprehensive legal framework for developing, commercialising, and using A.I. technologies. In the preamble, the bill expressly states that its provisions are based on the E.U. A.I. Act (recital 2), as evidenced by its risk-based approach.

Although the bill aimed to establish a framework for A.I. governance, it suffered from serious shortcomings. Its key concepts were left undefined, creating uncertainty

[145] Luca Belli et al., *AI Regulation in Brazil: Advancements, Flows, and Need to Learn from the Data Protection Experience*, COMPUT. L. & SEC. REV., Apr. 2023, at 1, 2 (U.K.).

[146] Cámara de Diputadas y Diputados de Chile, Proyecto de Ley No. 15869-19, Regula los sistemas de inteligencia artificial, la robótica y las tecnologías conexas, en sus distintos ámbitos de aplicación, [Regulates artificial intelligence systems, robotics, and related technologies in their various areas of application] (Apr. 24, 2023), (Chile), https://www.camara.cl/legislacion/proyectosdeley/tramitacion.aspx?prmID=16416&prmBOLETIN=15869-19&utm_source=chatgpt.com.

about the scope and meaning of its provisions. It also failed to engage with existing regulatory regimes, such as those for data protection and consumer protection, leaving significant intersections unexplored. Most strikingly, it introduced a rigid approval process for A.I. systems that applied across the board, with no attempt to differentiate among types of systems or contexts of use. This parliamentary motion proposed the creation of the National Artificial Intelligence Commission (art. 5) with functions that include evaluating authorisation requests from A.I. developers, providers, and users; developing regulatory recommendations; preparing annual reports on A.I. systems; creating and maintaining an A.I. systems registry; and addressing serious incidents or malfunctions. A notable feature of this bill was that it mandated prior authorisation from the National Artificial Intelligence Commission before developing, commercialising, distributing, or using any A.I. system (art. 6). AI systems classified as unacceptable risk are ineligible for authorisation. In contrast, high-risk A.I. systems may be approved if they meet specific requirements, such as risk management plans or input data management plans.

On 29 May 2024, this bill was formally consolidated with Bill No 16,821-19,[147] an executive initiative on the regulation of A.I. systems submitted to the National Congress. The resulting unified proposal adopts a horizontal approach, reflecting the Ministry of Science's announcement of an updated version of the National Artificial Intelligence Policy.[148] The consolidated bill is currently under consideration before the Chamber of Deputies.[149]

In its preamble, the Executive Branch bill references several key documents and efforts: UNESCO Readiness assessment methodology: a tool of the Recommendation on the Ethics of Artificial Intelligence; the updated National Artificial Intelligence Policy; the work carried out by the Senate's Commission on Future Challenges, Science, Technology,

[147] Cámara de Diputadas y Diputados de Chile, 372ª Legislatura Proyecto de Ley No. 16821-19, Regula los sistemas de inteligencia artificial, la robótica y las tecnologías conexas, en sus distintos ámbitos de aplicación,[Regulates artificial intelligence systems, robotics, and related technologies in their various areas of application] (May 7, 2024), (Chile), https://www.camara.cl/legislacion/proyectosdeley/tramitacion.aspx?prmID=17429&prmBOLETIN=16821-19.

[148] This instrument outlines AI guidelines, directives, and principles through 70 priority actions and 185 public service initiatives, primarily targeting social, economic, and educational aspects across public and private sectors. *See* Franco Giandana Gigena et al., Regulatory Mapping on Artificial Intelligence in Latin America: Regional AI Public Policy Report (2024).

[149] *See Chile lanza una política nacional de IA y presenta un proyecto de ley sobre IA siguiendo las recomendaciones de la UNESCO*, [Chile launches a national AI policy and presents a bill on AI following UNESCO recommendations], UNESCO (May 4, 2024), https://www.unesco.org/es/articles/chile-lanza-una-politica-nacional-de-ia-y-presenta-un-proyecto-de-ley-sobre-ia-siguiendo-las.

and Innovation in 2023 on A.I. topics, which convened a technical working group;[150] and the existing consensus, following the model of the E.U. A.I. Act, on the need to adopt a risk-based approach to the regulation of technologies based on A.I. systems. Nonetheless, the proposal is commonly seen as drawing on the E.U. A.I. Act as a reference point, while emphasising a more pronounced ex post regulatory approach that allows for flexibility, self-regulation, and experimentation in AI development.[151]

The bill comprises 31 Articles, and a transitory chapter contains four articles. The general provisions include definitions such as "Artificial Intelligence System", "risk", and "significant risk", identifying "the stakeholders involved in the A.I. cycle, from developers and vendors to users".[152]

The new draft law establishes several principles for A.I. systems, including human intervention and oversight; technical robustness and safety; data privacy and governance; transparency and explainability; diversity; non-discrimination and fairness; social and environmental well-being; accountability and responsibility; and the protection of consumer rights. A.I. systems are classified by risk level: Unacceptable Risk A.I. systems, which are prohibited due to incompatibility with fundamental rights; High-risk A.I. systems, which can negatively impact health, safety, fundamental rights, the environment, and consumer rights; Limited-Risk A.I. systems, which present no significant risks; and No Apparent Risk A.I. systems, which do not fall into the previous categories. High-risk systems must meet stringent requirements for risk management, data governance, technical documentation, record-keeping, accuracy, cybersecurity, transparency, human oversight, and post-market monitoring.

5.2.2. THE GOVERNANCE FRAMEWORK

The Executive Branch bill provides a different institutional framework, including the establishment of an A.I. Technical Advisory Council (art. 14). This consultative body will advise the Ministry of Science, Technology, Knowledge, and Innovation on the development, promotion, and continuous improvement of A.I. systems. This council,

[150] Ministerio de Ciencia, Tecnología, Conocimiento e Innovación (Chile), *Proyecto de ley que regula los sistemas de IA,* [Draft bill regulating AI systems], MinCiencia, (Chile), https://www.minciencia.gob.cl/areas/inteligencia-artificial/Inteligencia-Artificial/Proyecto-Ley-regula-sistemas-IA/.

[151] *See* Carolina Aguerre, *supra* note 141. *See also* Josefina Lira, *Regulación versus innovación: ¿Está en riesgo el desarrollo de la IA en Chile?*, [*Regulation versus Innovation: Is the Development of AI in Chile at Risk?*] Pontificia Universidad Católica de Chile (Aug. 11, 2025), https://www.uc.cl/noticias/regulacion-versus-innovacion-esta-en-riesgo-el-desarrollo-de-la-ia-en-chile/.

[152] Franco Giandana Gigena, *supra* note 148, at 68.

composed of representatives from the public and private sectors, as well as academia, will play a crucial role in identifying A.I. systems that pose high or limited risks and providing guidance on the regulatory framework for their operators. Additionally, the council will be instrumental in formulating guidelines for creating controlled test environments and setting compliance and accountability standards.

In parallel, the proposal states that the newly established Personal Data Protection Agency (created under Law No. 21,719, enacted in December 2024, that amends and substantially reforms Chile's 1999 data protection law) will oversee and ensure compliance with the A.I. law (art. 19). This assignment of enforcement powers to the Data Protection Agency is particularly noteworthy, considering its contentious status during the parliamentary discussions on amending Chile's Personal Data Law. The A.I. bill acknowledges the critical importance of data governance in developing and deploying A.I. systems. In its preamble (I. Foundations, 6. Specialised Institutions), the draft bill highlights that the choice of the authority responsible for monitoring and enforcing sanctions under the A.I. law is based on the understanding that any A.I. system's operation relies on data.

However, establishing the Personal Data Protection Agency presents several challenges. The agency is slated to commence operations in October 2026 (Transitory Article Four of Law No. 21,719), with full implementation expected by December 2026. As of now, the agency is not yet operational, and its capacity to effectively oversee A.I. governance is uncertain. The agency's mandate primarily focuses on data protection and privacy, and it lacks specialisation in areas such as product safety or AI system assessment. Consequently, its expertise may be limited to data governance issues, potentially hindering its ability to oversee A.I. systems comprehensively.

Moreover, the lack of established capacity raises concerns about its readiness to enforce the A.I. law effectively upon its commencement. While the integration of data governance into A.I. oversight is commendable, the agency's current limitations may impede its ability to fulfill this expanded role. Therefore, careful consideration must be given to the agency's capacity-building and potential collaboration with other specialised bodies to ensure effective A.I. governance.

Chile's A.I. governance model reflects a cautious yet evolving institutional strategy that remains in flux due to broader regulatory dependencies, most notably, the creation of a dedicated Data Protection Agency. While the Executive Branch's draft law signals a shift from a centralised authorisation regime to a more consultative, risk-based oversight structure, it leaves key enforcement mechanisms contingent on ongoing debates over the country's data protection framework. The reliance on the future supervisory authority introduces legal and institutional uncertainty, particularly as the Data Protection Agency is expected to assume a dual mandate over personal data processing and A.I. system compliance. This layering of responsibilities reflects a growing convergence between A.I. and data governance, but may also raise operational and legitimacy concerns without a clearly defined institutional architecture. Moreover, the fragmented approach, featuring an advisory council and an independent agency, could prove challenging in practice if coordination mechanisms are not robustly implemented. As such, Chile's regulatory trajectory underscores the importance of integrating A.I. oversight into existing and emerging data governance ecosystems while ensuring that supervisory bodies are adequately equipped, both legally and structurally, to engage with the evolving complexities of algorithmic accountability.

CONCLUSION

The European Union's A.I. Act is increasingly recognized as a normative reference point in transnational discourse on artificial intelligence governance. Although its drafters intend to exert some degree of international influence, the transboundary impact of the regulation beyond European borders, particularly in regions such as Latin America, should not be presumed to involve straightforward replication. Instead, a pattern of selective adaptation emerges, mirroring the earlier diffusion of E.U.-style data protection frameworks across the region. This suggests that the adoption of the AI Act is mediated by both the normative gravitas of the E.U.'s regulatory paradigm and the specific local constraints that shape its reception.

In this context, data governance emerges as a crucial aspect of regulatory alignment. This research highlights that data protection frameworks are not merely related to A.I. regulation; they form its legal and normative basis. This is particularly evident in Latin America, where many jurisdictions have already adopted European-style data protection standards, though adapted to their unique social and institutional apparatus. These existing frameworks provide a familiar legal structure for regulators and stakeholders, making it easier to engage with the A.I. Act's underlying logic. However, it should be kept in mind that, unlike data protection regulations, the regulation of A.I. is strictly connected to a broader discourse of governance, which must inevitably be read in the context of that specific country (or region) in the global A.I. race.

Structural similarities between the E.U.'s data protection framework and the A.I. Act strengthen the attractiveness (and to some degree, the practicality) of aligning with the E.U. model. Both systems target similar categories of actors, impose restrictions on data-driven practices, and promote a regulatory ethos focused on rights protection, transparency, and market accountability. These common features are significant; they help position A.I. governance as an extension of data governance rather than a completely distinct domain the E.U.'s data protection regime introduced a coercive element that is less evident in the A.I. Act. Specifically, the D.P.D. and G.D.P.R. incorporate mechanisms that encourage third countries to amend their laws to align with E.U. standards in return for benefits such as unrestricted access to the E.U.'s internal market. This "transactional" or "coercive" dimension,[153] in which countries modify their laws to gain or avoid specific regulatory advantages, is significant for the global diffusion of the E.U.'s data protection framework. The recognition of third-party legal regimes as "adequate" serves as an incentive for countries to harmonise their regulations, facilitating cross-border data flows. In contrast, the E.U. A.I. Act does not explicitly incorporate such coercive mechanisms. While the Act promotes alignment through its risk-based framework and regulatory principles, it lacks the same clear leverage for encouraging third-party jurisdictions to adopt similar laws. This represents the major difference with the E.U. data protection regime and the designation of G.D.P.R. as the gold standard[154]. At the same time, the A.I. Act serves as the first comprehensive regulation on A.I.

The A.I. Act also introduces institutional sophistication, complicating its external translation. Its risk-based, sector-sensitive design resists easy transplantation, functioning more as a flexible regulatory prototype than a turnkey model. Nowhere is this more evident than in its supervisory architecture. The Act envisages a multi-level enforcement structure involving national authorities, market surveillance bodies, and the newly established European Artificial Intelligence Office within the E.U. This model reflects the layered character of E.U. governance and its internal fragmentation.

For Latin American countries, these institutional complexities pose a significant challenge. As this research has shown, the A.I. Act implicitly sets out three potential pathways for institutional design: the establishment of new, dedicated A.I. agencies; the

[153] Greenleaf, *supra* note 30, at 3.

[154] *See* Giovanni Buttarelli, *The EU GDPR as a Clarion Call for a New Global Digital Gold Standard*, 6 Int'l Data Priv. L. 77 (2016) (U.K.); *see also* Alessandro Mantelero, *The Future of Data Protection: Gold Standard vs. Global Standard*, Comput. L. & Sec. Rev., Apr. 2021, at 1 (U.K.), where it is argued that more than GDPR as global standard it should be considered Convention 108 and its modernised version (Convention 108+) providing "a solution that is good enough and workable in many different contexts, without necessarily reaching a gold standard".

designation of existing bodies as competent regulators; or the creation of hybrid "competence centres" that combine centralised expertise with sector-specific knowledge. Each option has distinct implications regarding regulatory coherence, thematic alignment, and administrative capacity. Importantly, this is not simply a legal question: institutional design choices hinge on pragmatic considerations, including budgetary constraints and the maturity of existing oversight bodies.

Despite an early wave of regulatory initiatives to govern artificial intelligence systems across Latin America, the region has yet to produce comprehensive legislation comparable to the European Union's A.I. Act. Several interconnected factors explain this regulatory gap. First, the E.U.'s legislative framework reflects institutional arrangements and governance structures that may not readily translate to Latin American legal and political contexts, requiring substantial localization efforts. Second, Latin American nations, operating as emerging economies with strong growth imperatives, prioritize harnessing A.I.'s potential for economic development and technological progress. This developmental focus creates tension with comprehensive regulatory approaches that might be perceived as constraining innovation and competitive advantage in the global A.I. landscape. Against this backdrop, Brazil and Chile illustrate divergent trajectories that reflect their respective legal traditions, regulatory configurations, and political economies. Brazil has opted for a sectoral and adaptive approach, leveraging existing agencies with domain-specific mandates and favouring soft law instruments over binding rules. While this allows for flexibility and incrementalism, it raises concerns about consistency and cross-sectoral coordination. Recent proposals in Chile envision an intersectoral advisory council complemented by the enforcement powers vested in the new Data Protection Agency. Both cases reveal institutional ambiguity, particularly concerning enforcement mandates and the ongoing construction or reform of regional data protection regimes.

These developments suggest that while the E.U.'s A.I. Act serves as a reference point, primarily through its risk-based logic, its supervisory architecture is unlikely to be reproduced wholesale. Instead, countries like Brazil and Chile appear to converge on hybridised governance arrangements that blend advisory, sectoral, and centralised functions. These configurations reflect domestic regulatory ecosystems and the political and institutional priorities shaping how A.I. governance is imagined and implemented.

The core question of our study, concerning the role of D.P. in the context of A.I. and situations where new specialised agencies are required, it does not lend itself to a straightforward, definitive answer. In Latin America, the choice between expanding D.P.A. responsibilities and establishing dedicated A.I. agencies should be guided by practical considerations, including institutional capacity, available resources, and democratic governance principles. Although the region has a relatively advanced data protection infrastructure that offers a strong basis for A.I. oversight, the complex, technical, and cross-sectoral nature of A.I. governance demands innovative institutional approaches.

Effective strategies will likely involve leveraging existing D.P.A. expertise while developing new coordination mechanisms that align with each country's unique institutional landscape. For example, large economies (Brazil, Argentina, Chile) with developed institutional capacity should expand D.P.A. mandates while creating specialised coordination mechanisms. Brazil's S.I.A. model provides the most sophisticated template for this approach. In the case of medium-sized countries, a specialised A.I. coordination authority should be established while maintaining strong cooperation agreements with D.P.As. Peru's centralised model could work for countries with strong digital transformation leadership.

Ultimately, Latin America's potential contribution to global A.I. governance may not lie solely in choosing between existing models but rather in pioneering adaptive, hybrid approaches. These should aim to balance technical expertise with democratic accountability and foster regional cooperation, thereby creating frameworks that embody the region's values while addressing the practical challenges of governing transformative A.I. technologies.

CONTRIBUTORSHIP STATEMENT

Saverino, R., Trigo Kramcsák, P., and da Rosa Lazarotto, B. jointly conceived the overall argument and structure of the article. Saverino, R. took the lead in drafting the introductory section and Sections 1–2 and the Conclusion. Trigo Kramcsák, P. took the lead in drafting Sections 3–4 and Section 5.2. Da Rosa Lazarotto, B. took the lead in drafting Sections 5 and 5.1. All parts of the manuscript were developed through extensive joint discussion and iterative revision among the three authors. All authors reviewed and revised the full manuscript for intellectual content, approved the final version, and agreed to be accountable for the work.

FUNDING DETAILS

This article is partially funded through the support that one of the authors receives from the project "Articulating Law, Technology, Ethics and Politics: Issues of Enforcement and Jurisdiction of EU Data Protection Law under and beyond the General Data Protection Regulation (ALTEP-DP)", funded by the Vrije Universiteit Brussel (VUB) Strategic Research Programme. The funder had no role in the design of the study, the analysis, or the decision to publish.

DISCLOSURE STATEMENT

The authors report there are no competing interests to declare.

DATA AVAILABILITY STATEMENT

Data sharing is not applicable to this article as no new data were created or analysed in this study.