Artificial Intelligence

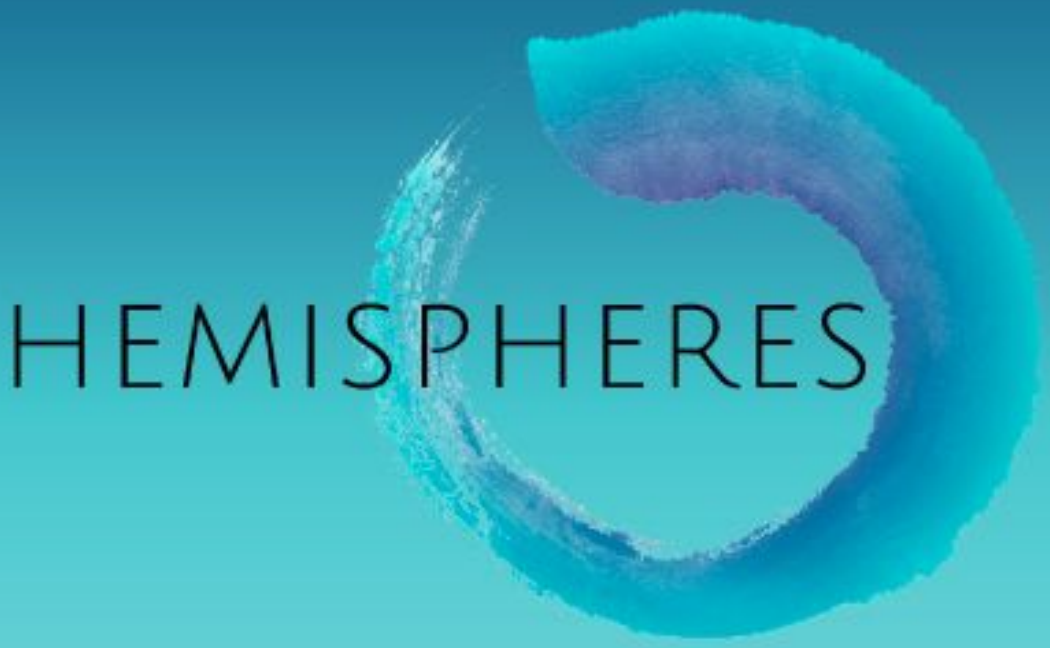
Emerging Technologies & Metaverse

Internet

Platforms, Equity & Safety

Privacy & Security

Youth & Media



Exploratory Policy Paper I October 2025

Privacy & Security

By Members of the Privacy & Security Working Group

Funded by the European Union

HEMISPHERES is funded by the ERASMUS-JMO-2024-NETWORKS Program.

Author(s)/Institution(s):

Ana María Castillo, Universitat Intern. de Catalunya
Urs Gasser, Technical University of Munich
Armando Guio Español, Network of Centers
Maria Pilar Llorens, Universidad de San Andrés
Christoph Lutz, BI Norwegian Business School
Maria Isabel Mejia Jaramillo, Universidad del Norte
Yamilet Serrano, Universidad de Ingeniería y Tecnología
Pedro Sigaud Sellos, Universitat Intern. de Catalunya
Fabro Steibel, ITS Rio

SUGGESTED CITATION

Castillo, A. M., Gasser, U., Guio Español, A., Llorens, M. P., Lutz, C., Mejia Jaramillo, M. I., Serrano, Y., Sigaud Sellos, P., & Steibel, F. (2025). *Privacy & Security.* HEMISPHERES. Technical University of Munich. https://hemispheres.digital/

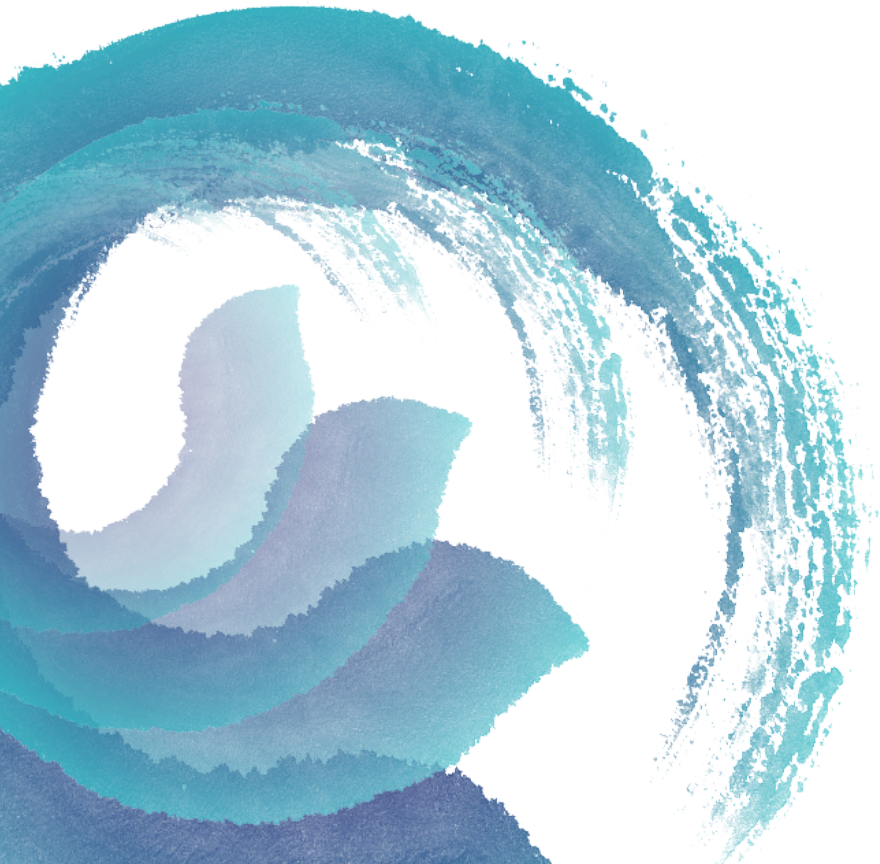


TABLE OF CONTENT

ABSTRACT

This exploratory policy paper reviews privacy and data protection regimes in the European Union (EU) and Latin America and the Caribbean (LAC), with particular attention to regulatory maturity, institutional architecture, and the development of adaptive governance tools. It uses the EU's comprehensive framework, grounded in the General Data Protection Regulation (GDPR) and independent DPAs, as a reference point, while acknowledging LAC's rights-based traditions, notably constitutional habeas data provisions. The analysis underscores shared institutional vulnerabilities, including underfunded and politically dependent DPAs, and highlights the role of regulatory sandboxes as experimental governance mechanisms. By mapping cross-regional convergence and divergence, the paper demonstrates how EU's procedural maturity and LAC's constitutional and citizen-centered innovations together create a fertile ground for reciprocal learning, regulatory pluralism, and globally relevant privacy governance.

This exploratory paper is a product of HEMISPHERES, an international collaboration exploring technology, policy, and regulation across the EU and Latin America and the Caribbean. It represents the culmination of a joint effort by a Working Group of academics from both regions, reflecting the rich diversity of their experiences and opinions. While individual contributors express their views in a personal capacity and may not agree with every statement, they are united by a shared commitment to fostering mutual learning between these distinct regulatory landscapes.

1. INTRODUCTION

In the era of big data and the emergence of new technologies, such as artificial intelligence (AI), the need for robust and context-sensitive data protection frameworks has never been more urgent. Across Latin America and the Caribbean (LAC) and the European Union (EU), societies are confronting a shared imperative: how to govern data in ways that safeguard fundamental rights, foster innovation, and preserve democratic accountability. Yet while both regions face similar challenges, their institutional trajectories, legal cultures, and governance models differ significantly, offering a fertile ground for mutual learning and transregional cooperation.

The Privacy and Security Working Group, established under HEMISPHERES, aims to bridge the gaps between these regional experiences. Its central purpose is to advance structured dialogue and joint research that promote convergence in data protection and governance[1]. This initiative recognizes that no region can tackle digital sovereignty, regulatory fragmentation, or platform accountability in isolation. Rather, it is through transregional engagement, grounded in respect for local contexts and informed by each other's innovations, that more resilient and adaptive governance models can emerge.

Particularly, this report aims to answer the question of how data protection is regulated in both regions and whether points of convergence or divergence can be identified on this topic. To do so, the report is organized in three main sections. The first section presents the state of data protection regulation. It emphasises that, although LAC has been strongly influenced by the EU regulations, the region is not merely copying them; rather, is adapting these frameworks to local realities.

The second section explores convergence between LAC and the EU on data protection, addressing topics such as the regulatory frameworks of data protection authorities (DPAs), the regions' capacity for innovation, novel approaches to regulation (such as regulatory sandboxes), and trust in regulatory institutions. This section underscores that truly independent DPAs are crucial for effective data protection, and that this effectiveness is closely tied to institutional

[1] In this report the group is not addressing cybersecurity issues.

maturity, legal clarity and inter-agency coordination. Moreover, it highlights that regulatory sandboxes are becoming consolidated as a strategic tool for adaptive governance and that there is room for potential mutual learning in this area.

Finally, the third section explores three areas for strategic collaboration between regions: data sovereignty, dark patterns concerns, and privacy by design. It highlights that these are promising areas for cooperation between EU and LAC, and that each region could potentially benefit from the other's experience.

2. NORM DIFFUSION AND LEGAL BORROWING

EU influence on LAC data protection regulation can be traced back at least, to the 1990s with the adoption of the Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data. At that time, LAC constitutional protection of habeas data was complemented with more comprehensive legislation imitating the European protections. Two distinct waves of legislation can be identified during this period. The first refers to legislation enacted immediately after the adoption of the Directive 95/46/EC, such as those passed by Chile in 1999 and Argentina the following year. The second wave occurred around 2010, when several LAC countries adopted data protection laws, for example Peru in 2011 and Colombia in 2012 (Carrillo & Jackson, 2022, Voss & Castes-Renard, 2016). This EUinfluence has become even more significant – both directly and indirectly – since the adoption of the General Data Protection Regulation (GDPR) in 2016. Since then, a third wave of legislation has emerged, in which LAC countries have adopted more comprehensive legal frameworks resembling the EU model. A prominent example from this wave is Brazil's General Data Protection Law (LGPD) adopted in 2018.

EU influence in LAC legal frameworks can be either direct or indirect. Direct influence involves an explicit acknowledgement by LAC lawmakers of GDPR's impact on drafting of national legislation. While indirect influence occurs when factors other than the GDPR drive the adoption of national data protection legislation.

LAC data protection legal frameworks show two forms of direct influence. The first occurs when national legislation recognizes the GDPR as its model or source of inspiration. In this regard, several LAC countries acknowledge some degree of influence from the GDPR in their drafting processes. Examples include draft bills in both Argentina and Colombia, which explicitly identify the GDPR as the 'standard to emulate' or a source of inspiration. The second form arises when local laws incorporate specific GDPR provisions. Relevant examples include: the extraterritorial reach and application of local legislation (e.g., Brazil); the obligation to conduct Data Protection Impact Assessments (DPIAs) (e.g., Brazil); the requirement to designate Data Protection Officers (DPOs) (e.g., Brazil and Chile); and the right to withdraw consent (e.g., Chile).

Several factors beyond the GDPR itself contribute to the adoption of the EU data protection standards in LAC. These factors can be labelled as indirect influence. For example, both LAC and EU recognize the right to privacy as a fundamental human right, making the GDPR an attractive standard for LAC countries to follow in this area. Additionally, compliance with the GDPR facilitates cross-border data flows, which motivates LAC countries to align their legislation with what are perceived as global standards.

As a result, the GDPR serves as an important reference for data protection processes in LAC countries. At first glance, it seems that the region's adoption of GDPR standards is more of a pragmatic approach than a result of careful consideration.

2.2. Mutual Learning in Data Protection: LAC's Strategic Experimentation and the EU's Normative Formalism

The development of data protection frameworks presents a valuable opportunity for mutual learning between LAC and the EU. While the EU has pursued a formalistic and normative approach – aiming to establish a global benchmark through the GDPR – LAC countries have adopted a more pragmatic and context-sensitive stance. This contrast underscores the potential for two-way regulatory exchange, where LAC's adaptive strategies can inform and challenge the EU's efforts toward universal standard-setting.

Although the Brussels Effect provides a useful lens to understand the diffusion of EU data protection norms, the regulatory landscape in LAC is shaped by more intricate and dynamic drivers. As Schwartz (2019, p. 803) notes, the EU has succeeded not only in producing a legally transplantable model but also in exporting conceptual frameworks that resonate in the global marketplace of ideas. Yet, LAC does not passively receive these models – it actively reshapes them.

LAC data protection laws, while clearly inspired by EU precedents, exhibit a high degree of normative autonomy. Rather than engaging in direct legislative transplantation, countries in the region recalibrate the GDPR's principles to fit their distinct constitutional, legal, and socio-political contexts. A salient example is the regional treatment of the "right to be forgotten." Unlike in EU, where it is

grounded in individual privacy and reputational control, in LAC it often clashes with deeply entrenched rights to truth and public memory – particularly relevant in societies emerging from authoritarian rule or conflict. This divergence illustrates the risks of “copy-paste” legislation that disregards contextual particularities.

LAC’s iterative experimentation with the GDPR – through selective incorporation, legal innovation, and normative balancing – offers valuable lessons for global data governance. It highlights the importance of regulatory flexibility, cultural embeddedness, and democratic legitimacy in building effective data protection regimes. Conversely, the EU can benefit from these adaptive practices as it seeks to promote globally resonant standards that are not only legally sound but also contextually viable and normatively inclusive.

2.3. Main Findings

- **EU Data Protection Standards Have Strongly Influenced LAC Frameworks—Both Directly and Indirectly**

  The EU's regulatory model, particularly the GDPR, has served as a key reference point for LAC data protection legislation across three distinct waves since the 1990s. This influence manifests both directly – through explicit references to the GDPR and adoption of its provisions, such as DPIAs, DPOs, and extraterritorial reach – and indirectly, through shared commitments to privacy as a fundamental right and the pragmatic incentive to facilitate cross-border data flows.

- **LAC Is Not Merely Imitating EU but Adapting Its Frameworks to Local Realities, Creating Opportunities for Two-Way Learning**

  While inspired by the EU, LAC countries strategically tailor GDPR-like rules to align with their constitutional traditions and social priorities. For instance, tensions between the EU's "right to be forgotten" and LAC's emphasis on the "right to truth" demonstrate how transplanting foreign legal norms requires cultural adaptation. This pragmatic, experimental approach offers valuable lessons for the EU, highlighting the importance of flexible, context-aware policymaking in the global governance of data.

3. LAC–EU CONVERGENCE ON DATA PROTECTION

Building on the preceding analysis of how both regulatory frameworks have interacted and mutually shaped the evolution of data protection norms, this

section turns to the critical challenges that remain. It identifies key areas where regulatory authorities in LAC and the EU face common tensions – and where meaningful collaboration is both possible and necessary. By examining the most salient regulatory frictions and institutional bottlenecks, this section aims to lay a foundation for a more structured and actionable cross-regional dialogue, one capable of transforming shared obstacles into opportunities for mutual learning, capacity building, and normative innovation.

3.1. Institutional Architecture

A robust analysis of privacy must begin with the institutional architecture responsible for its implementation and enforcement. Privacy protections depend not only on the substantive content of laws and regulations but also on the effectiveness of the institutions tasked with interpreting, overseeing, and enforcing those norms. These institutions – ranging from data protection authorities to sector-specific regulators and judicial bodies – serve as the operational backbone of privacy governance.

Focusing on institutional architecture provides critical insight into the conditions that enable or hinder effective privacy protection. Factors such as institutional independence, technical capacity, inter-agency coordination, and access to resources often determine whether privacy rights are upheld in practice or remain merely aspirational. By examining these institutional dimensions at the outset, the analysis is grounded in the practical realities that shape privacy governance in these countries. This approach highlights the need for coherent, capable, and context-sensitive regulatory frameworks – particularly in regions where institutional fragmentation or limited oversight capacity continues to challenge the realization of privacy as a fundamental right in both regions.

3.1.1 Creating and Sustaining Independent Data Protection Authorities

Data protection regimes in both LAC countries and the EU emphasize the importance of independent supervisory authorities as guardians of privacy rights. The EU's GDPR mandates that each member state maintain an independent data protection authority (DPA) insulated from external influence, reflecting a hard lesson that effective enforcement requires autonomy from political control. LAC

has followed suit in recent years, inspired by EU frameworks, with countries such as Brazil establishing dedicated data protection authorities and Panama strengthening the role of its existing authority.

Despite broad consensus on their importance, creating and sustaining truly independent DPAs has proven challenging on both sides of the Atlantic. In LAC, some early privacy laws focused on rights and principles but did not create separate regulators, resulting in gaps in enforcement independence (Chavarría-Mora, 2025). Even where authorities exist, their institutional design varies: several LAC DPAs are dual-purpose agencies that oversee both freedom of information and data protection (for instance, Argentina's AAIP, Mexico's former INAI, and Panama's ANTAI each began as transparency bodies later tasked with privacy enforcement). Operating with tight budgets and personnel, these hybrid agencies must balance open-government mandates with privacy oversight, a situation that can strain their focus and credibility.

By contrast, EU DPAs are typically specialized solely in data protection and cooperate through the European Data Protection Board (EDPB) to ensure consistent cross-EU application of the GDPR. This specialization helps sharpen their focus, though it also requires strong coordination mechanisms to handle cross-border cases effectively. Each model carries trade-offs: LAC's integrated approach can embed privacy values within broader governance but risks diluting regulatory attention, while EU's networked independence demands diligent coordination to tackle multinational data flows.

Both regions face shared tensions in maintaining DPA independence against political and institutional pressures, highlighting the need for constant vigilance in institutional architecture. EU law confers DPAs with legal guarantees of autonomy, yet even in the EU there have been instances where governments tested these boundaries, prompting EU court judgments to enforce strict independence and the EU Commission's scrutiny of national laws that fall short. In LAC, ensuring de facto autonomy can be even more precarious. Recent events illustrate this fragility: in Mexico, a 2024 constitutional reform abolished its autonomous transparency and data protection institute, transferring all data oversight functions to a government ministry. Such moves, which effectively negate independent scrutiny, have alarmed observers and civil society, underlining how political shifts can undermine regulatory institutions.

The lesson emerging from both continents is that a strong political culture and public support must buttress legal provisions for independent authorities. LAC authorities, such as Mexico's former INAI, have actively promoted a "data protection culture" to emphasize their role as impartial guardians of citizens' rights, and European DPAs similarly rely on public trust to defend their remit. In sum, building and sustaining independent DPAs is an ongoing challenge that unites the EU and LAC – one that requires not only robust laws but also continual reinforcement of those agencies' autonomy and authority in practice.

3.1.2 Budget, Political Autonomy, and Enforcement Capacity

Even the most comprehensive legal frameworks for data protection can be rendered ineffective in the absence of strong institutional capacity. A persistent and shared challenge in both LAC and the EU is the critical under-resourcing DPAs. In the EU, more than 80% of national DPAs have reported that their budgets are insufficient to fulfill their statutory mandates, and over 86% cite inadequate staffing levels to manage the increasing complexity and volume of GDPR-related responsibilities. These deficiencies have tangible consequences: backlogs in complaint handling, delays in investigations, and limited capacity to monitor compliance effectively. LAC regulators face similar, and often more acute, constraints, particularly as many legal regimes in the region are more recent and lack institutional maturity.

Closely intertwined with budgetary concerns is the question of political autonomy. While the GDPR enshrines formal guarantees of independence for DPAs, funding mechanisms remain under the control of national governments or parliaments, opening the door to political influence. The European Data Protection Board and the European Data Protection Supervisor issued a rare joint warning in 2022, cautioning that budgetary shortfalls were threatening their ability to meet legal obligations under the GDPR. In response, they publicly urged budgetary authorities to increase appropriations—an extraordinary step that underscores the structural tension between legal independence and financial dependency.

In LAC, these pressures are even more pronounced. Many DPAs operate within executive branch agencies or transparency bodies and are susceptible to administrative restructuring, which can dramatically impact their budgets and

staffing. The 2024 dissolution of Mexico's formerly independent DPA and its absorption into a government ministry serves as a stark example of how political shifts can dismantle institutional independence. Without stable funding, tenure protections, and a degree of operational autonomy, regulators struggle to enforce privacy rights, especially in politically sensitive or high-stakes cases involving powerful public or corporate actors.

Enforcement capacity, while still uneven across both regions, has shown signs of gradual development – driven in part by regulatory cooperation and shared learning. In the EU, a number of DPAs have built substantial enforcement track records under the GDPR, issuing high-profile fines and orders. Others, however, lag behind, often constrained by limited resources or the jurisdictional complexities introduced by the one-stop-shop mechanism. This mechanism, which delegates lead enforcement for multinational cases to the DPA of the company's main establishment, has generated friction and perceived bottlenecks, particularly in high-stakes cases handled by the Irish authority.

LAC, by contrast, is in the early stages of enforcement evolution, but notable progress is underway. Authorities such as Colombia's Superintendence of Industry and Commerce (SIC) and Brazil's National Data Protection Authority (ANPD) have begun to issue fines, publish compliance guidance, and experiment with new governance models. For instance, in 2020, Colombia's SIC launched a regulatory sandbox centered on privacy-by-design for AI systems; in 2023, Brazil's ANPD initiated a public call to develop a sandbox on AI and data protection—an innovative step toward aligning emerging technologies with fundamental rights.

Such developments are promising, but they also reveal the structural limitations many DPAs still face. Agencies across LAC often lack sufficient political backing and operational resources to impose meaningful sanctions or develop sustained enforcement strategies. These constraints are especially acute in jurisdictions where data protection is a relatively new policy area and where institutional legacies are still shaped by overlapping or competing governance mandates.

Importantly, enforcement must not be conceived solely in punitive terms. Proactive strategies that emphasize regulatory guidance, business education, and collaborative compliance can often yield better long-term results—particularly in environments where many organizations, especially SMEs, lack familiarity with

data protection obligations. Both EU and LAC regulators are increasingly recognizing the value of such approaches and are experimenting with cooperative tools, including public consultations, regulatory sandboxes, and co-regulatory frameworks.

Cross-border enforcement presents another critical challenge. While the GDPR provides a legal basis for extraterritorial reach, and some LAC countries are advancing toward alignment through regional standards and international conventions, meaningful interoperability remains limited. Divergent legal frameworks, procedural differences, and uneven institutional maturity make joint investigations and enforcement coordination difficult. To address these gaps, efforts such as the Ibero-American Data Protection Network (RIPD), which connects LAC regulators with their Spanish and Portuguese counterparts, have committed to shared capacity-building, technical training, and peer learning initiatives. Similarly, international platforms like the Global Privacy Assembly offer opportunities for global alignment on key enforcement challenges, including those posed by Big Tech and AI systems.

Looking forward, deeper cooperation between LAC and the EU will be essential to address these systemic barriers. Practical steps could include the development of shared protocols for managing cross-border data incidents, joint investigative task forces, and multilingual public reporting platforms to facilitate user complaints across jurisdictions. At the same time, regulatory peer exchanges, secondments, and harmonized guidance for SMEs could enhance compliance in ways that are sensitive to local institutional contexts.

Ultimately, effective data protection requires more than well-drafted statutes. It demands sustained investment in the institutional architecture of enforcement, a commitment to political independence, and international cooperation to address the transnational nature of today's data economy. Both LAC and the EU are beginning to converge around this realization, offering a fertile ground for mutual learning, policy innovation, and a more coherent global approach to safeguarding privacy.

3.2. Learning Lessons from EU Regulatory Maturity and LAC Innovation Capacity

EU's data protection architecture has attained a level of regulatory maturity that offers valuable lessons for LAC's evolving framework. The EU's experience stretches back to the 1995 Data Protection Directive and even earlier national laws since the 1970s, creating a continuum of jurisprudence, institutional knowledge, and procedural refinement leading up to the GDPR. The GDPR itself – implemented in 2018 – is widely seen as a global benchmark and has directly influenced privacy legislation far beyond EU. Its comprehensive scope and rigorous standards prompted many countries to re-examine their own laws; in LAC, the GDPR catalyzed a series of updates and new statutes to align with international best practices. EU regulatory maturity is evident not only in law but in institutional practices: mechanisms like the EDPB's consistency decisions, the cooperation among DPAs in cross-border cases, and the integration of data protection considerations into sectoral regulations (e.g. finance, health, telecommunications) have all been honed over years. LAC policymakers and regulators have actively studied these developments. For instance, Argentina and Colombia are in the process of overhauling decades-old data protection laws specifically to broaden individual rights and harmonize with modern EU standards. Such reforms draw on EU concepts – stronger consent requirements, accountability obligations for organizations, breach notification rules, etc. – demonstrating a cross-regional learning process where LAC leverages EU's hard-won regulatory insights to modernize its own legal landscape.

At the same time, LAC's approach to data protection showcases innovations and perspectives that can inform EU policy discourse, illustrating a two-way exchange. A distinctive feature of LAC data protection is its deep roots in constitutional and human-rights principles. Since the 1980s, many countries in the region have enshrined the right to habeas data in their constitutions, embedding personal data rights at the highest legal level (Carrillo and Jackson, 2022, Guadamuz, 2001). As of 2022, no fewer than 16 LAC countries had elevated data protection to constitutional status, reflecting a broad social consensus on the importance of informational self-determination. This rights-based foundation has spurred innovative legal tools – for example, the habeas data remedy (a judicial action to access or correct one's personal

information) was pioneered in LAC and prefigures the access and rectification rights now standard in laws worldwide (Chavarría-Mora, 2025).

LAC regulators have also often embraced a holistic view of information governance: by combining data protection oversight with transparency, open data, or even consumer protection roles, they approach privacy in context with other public interests. This can lead to creative policy solutions and closer alignment with citizens' daily concerns. Moreover, LAC's emerging regulatory strategies in the digital realm display a pragmatic blend of protecting rights while fostering innovation. Several countries are exploring flexible, experimental approaches – such as regulatory sandboxes for new technologies or multi-stakeholder forums – to address challenges like artificial intelligence in tandem with data protection. The emphasis on public engagement and social dimensions (for instance, ensuring data protection regulations help bridge digital inequalities rather than widen them) provides a valuable perspective that complements the EU's more formalized regulatory experience. These LAC innovations underscore that there is no one-size-fits-all model for data protection – and that diversity of approaches can be a strength, offering fresh ideas for safeguarding privacy in different societal contexts.

The shared journey of the EU and LAC in data protection illustrates a rich field of cross-regional learning, where each can benefit from the other's experiences and innovations. EU authorities, with their longer history, offer examples of institutional resilience and gradual improvements: for instance, EU's move from a patchwork of national laws to a harmonized regulation (GDPR) and its development of enforcement cooperation mechanisms could guide LAC in pursuing greater regional convergence. Indeed, LAC has already taken steps in this direction – the adoption of the 2017 Ibero-American Data Protection Standards provided a common set of principles and rights for the region, closely modeled on the GDPR to facilitate interoperable regimes. Such efforts mirror, at a voluntary level, the unity that EU law imposes, and they hold promise for easing cross-border data flows and raising baseline protections across Latin American and the Caribbean nations. Conversely, EU policymakers can glean insights from LAC's experiences, particularly the integration of data protection into broader governance and social policy frameworks.

The Latin American and the Caribbean focus on privacy as a social right – intertwined with transparency, anti-corruption, and digital inclusion – resonates with global debates about data ethics and equity (Lehuedé, 2019), potentially enriching EU's own discussions on emerging issues like artificial intelligence governance or the digital economy.

Furthermore, cooperation between the two regions is increasingly tangible. Countries like Argentina, Mexico, and Uruguay have engaged with EU institutions through adequacy dialogues and by joining international conventions (such as Council of EU's Convention 108), signaling mutual recognition of each other's standards. Joint initiatives, whether through the Global Privacy Assembly or bilateral exchanges, create channels for sharing best practices – for example, European DPAs mentoring newer LAC agencies on investigation techniques, or LAC regulators sharing strategies for public education and stakeholder engagement in diverse societies.

The institutional architecture of data protection in LAC and the EU, while shaped by different histories, faces common challenges and converging goals. By learning from one another – EU lending its regulatory maturity and LAC its spirit of innovation and rights-centric perspective – both regions can strengthen their data protection frameworks. This cross-regional dialogue and collaboration not only help address shared tensions in funding, independence, and enforcement, but also seize the opportunity to build a more coherent and adaptive global privacy regime that benefits individuals on both sides of the Atlantic.

3.3. Developing Privacy Regulatory Sandboxes

The development of regulatory experimentation spaces in privacy, particularly sandboxes, has become increasingly evident in both jurisdictions. While the global proliferation of sandboxes reflects a wider regulatory shift toward adaptive governance, the objective of this section is not to offer a comprehensive inventory of all existing initiatives. Rather, it focuses on a comparative analysis of those implemented in LAC and the EU, regions where regulatory sandboxes have been deployed with varying institutional rationales and legal traditions.

In the face of rapid technological change – including the rise of artificial intelligence, blockchain technologies, and 5G infrastructure – regulatory

sandboxes have emerged as critical policy instruments that allow regulators to engage with innovation in a controlled and iterative manner. They offer a structured environment for testing emerging technologies while safeguarding public interest, financial stability, and consumer rights.

A comparative overview of sandbox initiatives in LAC and the EU reveals differences in their institutional design, legal frameworks, and strategic focus. As summarized in Table 1 from the World Bank Group (2020), these differences are evident across several dimensions, including whether the sandbox is product- or policy-oriented, the length of the testing period, the type of regulating authority, and the legal system under which the sandbox operates. This comparative landscape provides not only a snapshot of regulatory diversity but also a valuable foundation for analyzing how sandboxes contribute to learning and adaptation in different governance contexts.

By closely examining selected cases from LAC and the EU, the following analysis aims to uncover the policy implications of these regulatory innovations and to identify opportunities for cross-regional learning.

Table 1: Overview of the Sandboxes in LATAM and EU (World Bank Group, 2020)

Country	Type of Sandbox	Testing Period	Legal System	Type of Regulator	Year
Barbados	Product	8 months	Common Law	Central Bank	2018
Bermuda	Product/Policy	not specified	Common Law	Central Bank	2018
Brazil	Product	not specified	Civil Law	Central Bank, Securities Regulator, Ministry of Finance	2020
	Product/Policy	3 months	Civil Law	Central Bank	2018
Bulgaria	-	not specified	Civil Law	Ministry of Finance	2020
Colombia	Product/Policy	not specified	Civil Law	Financial Sector Regulator	2019

Denmark	-	6-8 months	Civil Law	Financial Supervisory Authority	2019
Hungary	Product/Policy	not specified	Civil Law	Central Bank	2019
Jamaica	Product	Up to 24 months	Common Law	Central Bank	2020
Mexico	-	2 years	Civil Law	Central Bank, Financial Supervisor, Ministry of Finance	2019
Netherlands	Policy	Varies	Civil Law	Central Bank, Financial Supervisor	2017
Norway	Product	not specified	Civil Law	Ministry of Finance	2018
Poland	Product	not specified	Civil Law	Financial Supervisor	2018
Spain	Product	not specified	Civil Law	Ministry of Finance	2020

3.3.1 Convergences and Divergences in Regulatory Sandbox Experiences:

In LAC, regulatory sandboxes have developed as practical tools to manage technological change, particularly in fintech and data governance. Brazil and Colombia stand out for their proactive and iterative use of sandboxes not only to test innovative solutions but also to inform legal reform and institutional adaptation. Brazil's National Data Protection Authority (ANPD), for example, has launched an AI regulatory sandbox to support evidence-based enforcement of LGPD and to address the limitations of the existing legal framework in achieving algorithmic transparency. The sandbox enables the ANPD to engage directly with machine learning and generative AI systems, assessing how these technologies interact with privacy safeguards and data protection principles. This initiative coincides with the ongoing debate in Brazil's Congress over Bill 2338/2023, which aims to establish a national AI supervisory authority (Guio, 2024).

Colombia presents a similarly layered approach, having built its AI sandbox on the foundations of its earlier fintech sandbox, "laArenera," developed by the Superintendence of Finance (SFC). This earlier sandbox provided a structured space for testing financial innovations in a controlled regulatory environment, striking a balance between oversight and technological development. The AI sandbox, administered by the Superintendence of Industry and Commerce (SIC), extends this model by fostering compliance-by-design approaches among AI developers, particularly in relation to data protection. It provides non-binding regulatory guidance, aiming to ensure that AI systems are both innovative and respectful of fundamental rights, particularly in relation to data collection and usage (Guio, 2024). The process for participation is structured through a detailed application, requiring developers to demonstrate the innovation potential of their AI systems, the data used –including whether it involves minor – and their experience with similar projects in other jurisdictions (Superintendencia de Industria y Comercio, 2021, as cited in Guio, 2024).

In contrast, the EU's approach to regulatory sandboxes is more reserved and less harmonized. Although several member states such as the Netherlands, Spain, and Poland have independently established sandbox environments, there is no EU-wide mandate or binding framework guiding their implementation (World Bank Group, 2020). The EU AI Act only makes a marginal reference to sandboxes, suggesting that member states "may" introduce them, but offering no formal requirement or consistent operational criteria (Ringe, 2023; Guio, 2024). This results in a fragmented landscape where regulatory experimentation depends heavily on national discretion and lacks the systemic integration needed to shape continental-level governance. Furthermore, the absence of an "experimentation clause" within EU law – one that would allow temporary regulatory flexibility for the purposes of testing – limits the ability of regulators to engage dynamically with AI development in real-world contexts (Ringe, 2023).

The contrast between these two regions points to differing regulatory philosophies. In LAC countries, sandboxes are increasingly viewed not merely as tools to facilitate market entry, but as learning infrastructures that inform broader policy and regulatory development. In both Brazil and Colombia, sandbox experiences are explicitly used to refine legal standards and administrative functions, reflecting an understanding of regulation as an evolving and interactive process. These initiatives embody what Guio (2024) describes as "regulatory

reflexivity," in which experimental governance feeds directly into the legislative pipeline and institutional growth.

In the EU, however, sandboxes tend to operate more narrowly – often addressing isolated regulatory ambiguities or enabling limited experimentation under tightly controlled parameters. Without a regionally coordinated framework or strong political impetus to use sandbox insights for long-term legal reform, these experiments risk remaining disconnected from broader institutional transformation. The existing models, while operationally effective in some member states, lack the binding scaffolding to translate localized learning into EU-wide policy alignment.

Yet despite these divergences, both LAC countries and the EU face common implementation challenges. These include high administrative costs, the demand for technical expertise, and the need to ensure that sandbox-generated evidence leads to concrete policy outcomes. These shared hurdles underscore the value of cross-regional policy learning. LAC could benefit from the EU's more established regulatory infrastructure and potential for regional harmonization, while the EU could look to LAC countries' more flexible and participatory sandbox models as a blueprint for enhancing agility in digital regulation.

In sum, while both regions increasingly recognize the strategic value of regulatory sandboxes, they differ substantially in how these instruments are operationalized and embedded in their respective governance ecosystems. LAC's approach reflects a model of adaptive, rights-based experimentation closely linked to policymaking and institutional development. The EU, for its part, continues to treat sandboxes as optional mechanisms, constrained by regulatory formality and institutional inertia. Bridging this divide will require stronger political will, legal reform, and mechanisms to ensure that insights from regulatory experimentation translate into long-term governance improvements on both sides of the Atlantic.

3.4. Increasing—or Eroding—Stakeholder Trust in Privacy Rulemaking

The premise that regulatory frameworks can directly foster public trust in data protection and emerging technologies is both widely claimed and increasingly scrutinized (Tamò-Larrieux et al., 2024). EU and LAC policymakers alike often cite

trust as a central goal, whether through the GDPR's emphasis on transparency and accountability or LAC constitutional commitments to informational self-determination (Chavarría-Mora, 2025; De Hert & Lazcoz, 2022; Felzmann et al., 2019; Grisales Rendón, 2022). However, as recent scholarship highlights (Tamò-Larrieux et al., 2024), trust is a complex, relational phenomenon that cannot be fully engineered by law alone. Trust involves navigating uncertainty and vulnerability, and while regulation can mitigate some of these conditions (e.g., by limiting risks, increasing transparency, or establishing oversight mechanisms), it cannot eliminate them entirely. Thus, law can scaffold trust by shaping the conditions under which it can emerge, but it cannot guarantee trust in itself. The distinction between creating trustworthy systems and generating trust in those systems is important, especially when public attitudes toward digital governance are uneven or ambivalent.

This tension is particularly salient in the transregional context. In the EU, the GDPR aims to cultivate trust by mandating strong individual rights, independent oversight, and cross-border enforcement cooperation. Yet even in this mature regulatory ecosystem, public trust in digital institutions remains variable and sometimes fragile (Special Eurobarometer 487a, 2019). In LAC, where data protection regimes often derive from broader human rights traditions (Carillo & Jackson, 2022), trust-building efforts tend to foreground public engagement, transparency, and social justice concerns. These differences in emphasis suggest valuable cross-regional insights: EU can benefit from LAC's holistic, citizen-oriented approach to building legitimacy, while LAC regulators can draw on EU's experience in formalizing trust-enabling mechanisms like redress pathways and institutional independence. Ultimately, both regions face the challenge of avoiding overtrust, which may lead to complacency or misuse, and distrust, which can undermine compliance and public legitimacy (Aroyo et al., 2021; Lee & See, 2004; Passi & Vorvoreanu, 2022; Wagner et al., 2018). Rather than assuming that regulation alone can manufacture trust, policymakers must recognize that trustworthiness is cultivated through consistent, inclusive, and accountable governance - something that must be performed and perceived over time, not merely legislated.

3.5. Main Findings

Drawing on the above analysis of LAC–EU convergence in data protection, this section highlights the following key findings:

- **Institutional Design and Political Autonomy Are Foundational to Effective Data Protection**

  Both LAC countries and the EU face persistent challenges in establishing and sustaining independent, well-resourced data protection authorities (DPAs). Despite formal legal guarantees – especially under the GDPR – DPAs in both regions remain vulnerable to political influence through budgetary control and administrative restructuring. True autonomy requires more than legal status; it depends on stable funding, professional independence, and public trust in regulators' ability to enforce rights impartially.

- **Enforcement Capacity Is Uneven and Correlated with Institutional Maturity**

  The effectiveness of data protection enforcement varies widely within and across both regions. In the EU, some DPAs have developed robust enforcement records under the GDPR, while others lag behind due to structural and jurisdictional constraints. LAC regulators, though newer, are innovating with approaches like regulatory sandboxes and non-binding guidance to foster compliance-by-design. Across the board, enforcement capacity is closely tied to institutional maturity, legal clarity, and inter-agency coordination.

- **Regulatory Sandboxes Are Emerging as Strategic Tools for Adaptive Governance**

  Regulatory sandboxes have gained traction in both regions as mechanisms to manage technological innovation while safeguarding fundamental rights. However, their design and implementation diverge significantly: LAC countries like Brazil and Colombia are using sandboxes to actively inform legal reform and build institutional capacity, whereas EU member states have adopted more fragmented and formalistic approaches, lacking a harmonized framework or legal basis for experimentation. This asymmetry highlights the potential for mutual learning.

- **EU's Regulatory Maturity and LAC's Rights-Based Innovation Offer Complementary Strengths**

  The EU's long-standing data protection architecture provides a model of procedural consistency and institutional resilience. At the same time, LAC contributes unique strengths through its constitutional enshrinement of data rights, holistic integration with other policy domains (e.g., transparency and anti-corruption), and experimentation with public engagement tools. This cross-regional dialogue illustrates the value of pluralism in privacy governance and challenges the notion of one-size-fits-all legal transplants.

- **Building Trust in Privacy Rulemaking Requires More Than Legal Design**

  While both the GDPR and LAC frameworks aspire to foster public trust, recent scholarship underscores that trust cannot be engineered solely through regulation. It must be earned through transparent, inclusive, and accountable governance practices over time. Differences in regional emphasis – EU's focus on institutional mechanisms and LAC's attention to social legitimacy – offer valuable insights into how trustworthiness is cultivated and how trust itself remains a dynamic, context-dependent phenomenon.

4. STRATEGIC AREAS FOR TRANSREGIONAL COLLABORATION: TOWARDS A REGULATORY LEARNING APPROACH

Building on the institutional insights, enforcement challenges, and innovation pathways identified in the preceding sections, this final part of the analysis turns toward the strategic opportunities for transregional collaboration. While LAC countries and the EU operate under different legal traditions and levels of regulatory maturity, both regions are confronting parallel dilemmas in governing data protection and privacy. From institutional fragmentation and resource asymmetries to experimental regulatory tools such as sandboxes, it is clear that neither region can afford to address these challenges in isolation. Rather than viewing these differences as obstacles, they should be leveraged as assets in a shared regulatory learning process – one that embraces comparative strengths and fosters a more resilient and adaptive global privacy framework.

This section proposes a forward-looking agenda anchored in the concept of regulatory learning – a model of governance that values iteration, mutual observation, and cross-context adaptation. By identifying areas of convergence and divergence in current practices, and recognizing the distinct innovations developed in each region, LAC and the EU are well positioned to engage in more systematic knowledge exchange and joint problem-solving. In doing so, they can contribute to a more polycentric and inclusive model of tech governance, one that reflects diverse societal values while responding to global pressures for coherence, accountability, and rights-based oversight in the digital age.

4.1. Data Sovereignty and Regional Integration

Data sovereignty is not a straightforward notion. It has different meanings, nuances and connotations which vary according to context and to the sources consulted (see Hummel et al, 2021). In this report, data sovereignty is understood as the right of nations or regions to regulate how data is handled and transferred within their jurisdictions (Hutchison, Stilinovic & Gray, 2024).

From the perspective of LAC, digital sovereignty is deeply intertwined with the region's long-standing struggles for autonomy in governance, economic development, and technological innovation. Unlike the EU – where digital sovereignty is largely framed as a response to the dominance of foreign technology firms and as a mechanism for upholding democratic values – LAC presents a more fragmented and context-specific landscape. Each country pursues its own regulatory trajectory shaped by institutional capacity, political priorities, and varying levels of digital infrastructure. While the EU has developed a highly institutionalized framework aimed at asserting control over the collection, processing, and transfer of data related to its residents – through mechanisms such as data localization mandates, cross-border transfer restrictions, and stringent corporate accountability requirements (InCountry, 2025) – most LAC countries have historically taken a more laissez-faire approach to data governance. Nonetheless, this trend is beginning to shift.

For example, Peru does not have comprehensive data localization or residency laws, and there are generally no prohibitions on transferring data abroad. Nevertheless, in certain public procurement processes – particularly involving cloud services—Peruvian authorities may require data to be stored within the country for national security purposes (Baker McKenzie, 2025). In contrast, Argentina imposes more explicit data localization obligations through various sectoral rules. Although its Personal Data Protection Law No. 25,326 does not mandate data localization, other regulations require specific records, such as corporate books and tax documents containing personal data, to be stored at the company's legal domicile. Likewise, Central Bank regulations allow financial institutions to outsource IT services, provided that certain types of sensitive data remain stored domestically (Baker McKenzie, 2025).

Countries such as Brazil are advancing more comprehensive regulatory regimes that signal a growing commitment to asserting national control over data flows and aligning with global standards for data protection and digital sovereignty (Mejias, 2023). Brazil illustrates a nuanced approach to this agenda. While it does not impose broad-based data residency or localization requirements, targeted rules apply to specific categories of sensitive data – particularly in the public and financial sectors. For instance, the processing of classified government information or data related to the Federal Public Administration may require that such data be stored within national territory. Similarly, in the financial sector,

Resolution No. 4,893/2021 of the National Monetary Council does not mandate local storage for cloud-based data used by financial institutions. However, it imposes strict conditions to ensure regulatory oversight: institutions must guarantee the Brazilian Central Bank's access to the data. This can be achieved either through an international cooperation agreement with the jurisdiction where the data is stored or, in its absence, through the Central Bank's prior approval of the cloud services agreement (Baker McKenzie, 2025). This framework reflects Brazil's pragmatic approach – balancing the operational flexibility of cloud computing with sovereign control over critical data assets.

These regulatory differences underscore the region's legal heterogeneity and the importance of context-sensitive approaches to digital sovereignty. Rather than converging around a single model, LAC countries are navigating a complex regulatory patchwork, seeking to balance innovation, autonomy, and international cooperation in ways that reflect local priorities and institutional capacities. This fragmentation is interpreted in different ways. For some, it reflects a legitimate assertion of technology sovereignty. More specifically, technological sovereignty refers to the desire of a nation-state or supranational entity to influence and steer global sociotechnical systems, aiming ultimately to secure long-term economic prosperity and ensure the effective delivery and evolution of state functions for its population (Edler, J.et al, 2023). However, others emphasize that enabling cross-border data flows is essential to unlocking socioeconomic opportunities. Limiting such flows, they argue, could hinder economic progress and reduce the societal gains of digital transformation. In response, it is crucial for governments, regulators, the private sector, and civil society to move away from rigid data localization policies and instead pursue cooperative frameworks that support data mobility while safeguarding personal data and privacy rights (GSMA, 2017).

It is also important to distinguish between legal frameworks that explicitly promote data localization and those that impose restrictions on cross-border data flows. While these norms may have different underlying objectives – such as national security, privacy, or economic development – they can often result in similar outcomes. For this reason, it is essential to understand that restrictions on data transfers, even when framed as safeguards or adequacy requirements, may functionally serve the same purpose as localization mandates.

In this context, there are growing opportunities for international collaboration aimed at harmonizing standards and establishing shared principles for cross-border data governance. One notable example is the RIPD, which has undertaken significant efforts to promote regulatory convergence among national data protection regimes in LAC. These efforts include technical exchanges, structured regulatory dialogues, and the development of common standards for international data transfers (Red Iberoamericana de Protección de Datos, 2021).

Similarly, MERCOSUR has made meaningful advances in regional regulatory cooperation by promoting transparency and facilitating alignment among member states. The MERCOSUR Framework Agreement on Electronic Commerce, adopted in 2021, includes a dedicated section on the protection of personal data. It commits the parties to:

- Adopt or maintain laws, regulations, or administrative measures to safeguard users' personal data in electronic commerce, taking into account prevailing international standards;
- apply an adequate level of protection to personal data received from another MERCOSUR state, whether through national law, bilateral or multilateral agreements – general or sector-specific – or broader international frameworks, including contractual or self-regulatory instruments for the private sector;
- promote the adoption of security measures for personal data processing and inform users about their rights of access, rectification, and deletion;
- establish mechanisms to set common standards for personal data protection and enable its free flow within MERCOSUR.

With respect to cross-border data transfers, the agreement allows each party to retain or establish its own regulatory requirements, including those concerning personal data protection. However, it also obligates parties to authorize data transfers necessary for commercial activity between MERCOSUR states – provided that any restriction is based on a legitimate public policy objective and is not applied arbitrarily or in a manner that disguises trade barriers (Giay, G. P., et al, 2021)

These commitments gain further significance in light of the MERCOSUR–European Union Agreement, which seeks to deepen regulatory cooperation and enhance mutual understanding – not only among the parties themselves but also with EU institutions. European stakeholders have increasingly

recognized the alignment of these efforts with the EU's own strategic priorities. From an industry perspective, the agreement's chapter on telecommunications services is especially important. It affirms the independence of regulatory authorities and commits the parties to simplify licensing regimes, which could alleviate bureaucratic burdens in a historically over-regulated sector. Moreover, the agreement has the potential to foster regulatory learning and institutional capacity-building. By promoting the exchange of best practices and implementation outcomes, it can serve as a valuable platform to reflect on the evolving EU framework – particularly the Digital Services Act (DSA) and the Digital Markets Act (DMA) – and consider how analogous regulatory instruments might be adapted in LAC contexts (Blanco López-Alfaro and Barrionuevo, 2024).

There are, indeed, important lessons LAC countries can draw from the EU's regulatory trajectory. The DMA and the Data Governance Act (DGA), for instance, embody a comprehensive and enforceable vision for fair and interoperable digital markets, supported by strong public institutions. For LAC countries – where enforcement mechanisms are frequently under-resourced and institutional fragmentation persists – these examples can offer inspiration for addressing platform power, encouraging competition, and reinforcing public trust in digital services. However, wholesale adoption of EU legal models would be inappropriate. LAC policymakers must tailor these insights to the region's unique political economies, characterized by persistent informality, entrenched inequality, and uneven access to digital infrastructure.

A more productive and equitable path lies in fostering transregional regulatory learning. Rather than aiming for convergence around a single model of digital sovereignty, EU and LAC countries can benefit from collaborative frameworks that promote regulatory experimentation, mutual learning, and context-sensitive adaptation. LAC's emphasis on collective rights and community-based data governance – particularly in marginalized communities – offers valuable perspectives to ongoing EU debates on data justice and ethical stewardship. Conversely, the EU's institutionalized oversight structures and interoperable data-sharing mechanisms may assist LAC jurisdictions in building more robust, transparent, and adaptive digital governance systems.

Ultimately, forging bridges between these complementary models is essential for advancing a more inclusive and equitable global digital order – one that honors

local priorities while ensuring accountability, interoperability, and rights-based governance across borders. However, it is equally important to acknowledge the regulatory fragmentation that persists across the LAC region. This fragmentation is not limited to personal data protection laws but extends to sectoral regulations – including those governing health, public security, and taxation – which often operate in isolation and lack coherent integration. Recognizing and addressing these interdependencies will be critical to realizing the full potential of cross-border regulatory cooperation and fostering an effective, whole-of-government approach to digital governance.

4.2. Dark Patterns, Consent, and Platform Governance

Both the EU and many LAC countries are trying to address the growing prevalence of so-called dark patterns, which describe manipulative interface designs that nudge users into making privacy-intrusive choices, often without meaningful consent (Gray et al., 2018; Luguri & Strahilevitz, 2021). These deceptive practices undermine core principles of data protection, particularly transparency and user autonomy, and disproportionately affect vulnerable populations with lower digital literacy (Hilton, 2023; Zac et al., 2023). The GDPR requires informed consent to be freely given, specific, informed, and unambiguous. Yet in practice, consent is often rendered meaningless by platform design choices that obscure options, pre-tick boxes, or make it harder to reject than to accept data collection. In response, EU regulators and civil society organizations have started to push back. The Deceived by Design campaign by the Norwegian Consumer Council, for example, helped bring dark patterns into the spotlight, prompting enforcement actions and policy debates across the EU (Forbrukerrådet, 2018).

LAC countries, while at an earlier stage in regulating digital platform design, is well-positioned to contribute to this agenda through its strong consumer protection traditions and rights-based legal frameworks. Countries like Brazil and Mexico are already integrating consumer rights and data protection in their platform oversight strategies (Sombra, 2020; Velasco & Rascovsky, 2022). Moreover, LAC regulators and civil society actors have a track record of addressing informational asymmetries and platform power through constitutional rights such as habeas data. This creates a foundation for cross-regional collaboration in the form of sharing research, co-developing design standards,

and amplifying civil society initiatives aimed at banning manipulative design practices. A transregional approach could also target global platforms more effectively: joint advocacy, regulatory alignment, and shared enforcement actions may help counteract the structural power imbalance between tech companies and users in both regions. Ultimately, confronting dark patterns is not just about individual consent but about restoring fairness and agency in digital environments – a goal that resonates across borders.

4.3. Privacy by Design and Tech Regulation

Privacy by Design (PbD) mandates that data protection measures be integrated into the architecture of systems and services from their inception, rather than as an afterthought. The concept, formalized in GDPR Article 25, requires organizations to implement appropriate technical and organizational measures – such as data minimization, pseudonymization, and encryption – to ensure that, by default, only personal data necessary for each specific purpose is processed. For example, a mobile health app must encrypt data at rest and in transit, limit collection to strictly necessary health metrics, and disable automatic geolocation unless the user explicitly opts in (i.e., privacy “by default”).

In the EU, PbD is enshrined directly in the GDPR. This translates to organizations should build privacy into their projects from the very beginning, considering data protection during system architecture and software development, while collecting and retaining only the personal information needed for each purpose and, whenever possible, storing or processing it in pseudonymized or anonymized form. They must also implement technical and organizational safeguards, such as encrypting data at rest and in transit, utilizing privacy-preserving authentication methods, and enforcing strict access controls. Some recommendations include establishing clear accountability (e.g., a Data Protection Officer) to oversee privacy at all times. Conduct DPIAs for sensitive data or high-risk activities, noting potential issues and how you’ll address them. Use privacy-preserving technologies (such as advanced encryption or methods that allow data processing without exposing it). Always configure systems with the strongest privacy settings by default (e.g., disabling nonessential features unless the user opts in). Finally, keep audit logs and regularly review these measures to ensure they remain effective.

In this context, many LAC jurisdictions have taken inspiration from the GDPR when enacting or updating their data protection laws. However, the level of specificity and enforcement mechanisms varies significantly across the region. For example, Brazil follows the GDPR model and explicitly references PbD in its legal framework. Brazil's LGPD explicitly requires data controllers to implement "security, including privacy by design and by default" (Art. 6, IX). In October 2021, Brazíl's ANPD issued Resolution No. 4, which provides detailed guidelines emphasizing that organizations must document how PbD measures, such as data minimization, encryption, and access controls, are embedded from the start. More recently, ANPD's October 2023 regulatory sandbox for AI and data-driven projects mandates that applicants submit comprehensive PbD plans – including pseudonymization protocols and default privacy settings – before receiving any exemptions.

On the other hand, in other LAC countries such as Colombia, the concept of PbD has been informally integrated through Law 1581 of 2012 and its implementing Decree 1377 of 2013, which require data controllers to adopt strict security policies, such as access controls, encryption, and documented privacy notices, before processing any personal information. Although neither statute explicitly uses the term "Privacy by Design," the Superintendence of Industry and Commerce (SIC) established a regulatory sandbox in 2021 for AI projects that mandates developers demonstrate how privacy safeguards (e.g., pseudonymization protocols and minimal data collection) are built into their systems from the outset.

In Chile, the Personal Data Protection Law (LPPD) expressly incorporates "privacy by design and by default" as a core principle, requiring both public and private entities to embed technical and organizational measures—such as data minimization, DPIAs, and default opt-out settings—into every stage of product and service development. The LPPD also tasks the nascent Personal Data Protection Agency with issuing guidelines that mirror GDPR-like standards for PbD implementation, including mandatory documentation of privacy-preserving technologies and governance frameworks. Finally in Peru, while the Personal Data Protection Law (Peru's LPDP) and its updated Regulations (Supreme Decree No. 016-2024-JUS) do not explicitly reference "Privacy by Design," they embed PbD principles through requirements for data security, proportionality, and purpose limitation. Article 9 of Perú's LPDP requires controllers to implement "appropriate

security measures" to prevent unauthorized access, loss, or alteration of personal data, and the 2024 Regulations expand on this by mandating that organizations conduct risk assessments (akin to DPIAs) for high-risk processing and maintain documented policies on data retention, encryption, and access controls. Although Peru's framework lacks a direct PbD mandate, the emphasis on security and continuous monitoring effectively encourages organizations to consider privacy impacts from the earliest design phases.

In summary, while Colombia, Chile, and Peru have all incorporated Privacy by Design principles to varying degrees, Chile stands out for explicitly embedding PbD into its new Personal Data Protection Law, requiring clear guidelines and documentation from both public and private sectors. Together, these approaches reflect a regional trend toward harmonization with international best practices, offering a foundation for future regulatory refinement and greater interoperability across LAC privacy frameworks.

4.4. Main Findings

Although there are several areas where regulatory learning could be applied, the group selected three topics, and the key findings are highlighted below:

- **Nuanced Approaches to Data Sovereignty Are Necessary For Effective Collaboration Across Regions**

  Data sovereignty is not a straightforward notion; its meaning varies depending on the context and sources consulted. While the EU has highly institutionalized frameworks, LAC presents a more context-specific landscape and has historically adopted a more laissez-faire approach to data governance. As a result, the region is navigating a complex regulatory patchwork, seeking to balance innovation, autonomy, and international cooperation in ways that reflect local priorities and institutional capacities. Within this context, there are opportunities for international collaboration and learning.

- **Effectively Addressing Dark Patterns Will Require Coordinated Action**

  Dark patterns practices undermine core principles of data protection by rendering consent meaningless, thereby affecting transparency and user autonomy. LAC countries well-positioned to help address this problem, given its

experience in consumer protection and its rights-based legal frameworks. Additionally, the region could build on its history of addressing informational asymmetries. A transregional approach may offer a more effective way to tackle this issue.

- **Privacy by Design Is a Common Goal, but Its Implementation Varies Significantly Across and Within Regions**

  Privacy by design principles are enshrined in the GDPR, ensuring that privacy is considered from the very beginning of projects and that systems are configured with the strongest privacy settings by default. LAC countries seek to emulate GDPR standards in this area. However, the level of specificity and the strength of enforcement mechanisms vary significantly across the region. As a result, there is room for improvement and collaboration.

5. NEXT STEPS

Based on the debates held, the Working Group recommends the following next steps to move forward the discussions related to data privacy governance challenges.

1. **Address the intersection of data privacy and AI governance and regulation**

   AI and data are deeply intertwined. As a result, the Working Group considers it necessary to address concerns arising from this relationship and emphasises that this intersection should become a strategic area to be considered in future policy reports.

   The group identified several areas for further exploration: a) the growing influence of AI governance and regulation on traditional data protection legal frameworks; b) the need to understand how generative AI is shifting data protection paradigms; and c) the influence of AI deployment and usage on youth's attitude to data protection regulations, particularly their increased willingness to share personal data without fully considering the consequences.

2. **Map data privacy capacity and stakeholders**

   An essential step to better address challenges on data privacy governance and regulation is to map existing capacities and stakeholders. A comprehensive identification of key actors, institutions, regulatory frameworks, and capacity across EU and LAC states can support the development of more effective policy recommendations. This mapping will enable the Consortium to foster collaboration with relevant actors and leverage existing capacities across both regions.

3. **Build community of practice**

   Once key data privacy stakeholders are identified, the group recommends fostering a community of practice. This would help ensure that bottom-up privacy practices and 'on-the-ground' implementation are taken into account when designing policies.

4. **Consider the learning outcomes from data protection regulation evolution**

The group considers that the evolution of data protection regulation, and, more broadly, data protection governance, offers valuable insights for regulatory learning. In this context, the group suggests advancing on two areas: a) explore whether the evolution of data protection regulation could serve as the basis for regulatory learning in other areas under consideration by the Consortium; and b) examining how the evolution timeline of regulatory development influences the learning process

6. REFERENCES

Aroyo, A. M., De Bruyne, J., Dheu, O., Fosch-Villaronga, E., Gudkov, A., Hoch, H., ... & Tamò-Larrieux, A. (2021). Overtrusting robots: Setting a research agenda to mitigate overtrust in automation. Paladyn, Journal of Behavioral Robotics, 12(1), 423-436.

Baker McKenzie. (2025, January 3). Global Data and Cyber Handbook. Baker McKenzie. Retrieved June 20, 2025, from https://resourcehub.bakermckenzie.com/en/resources/global-data-and-cyber-handbook/latin-america/brazil/topics/data-localization-and-regulation-of-non-personal-data

Blanco López-Alfaro, A., and Barrionuevo, P. (2024, 19 de diciembre). El Acuerdo Unión Europea–Mercosur: una oportunidad única [Entrada de blog]. Telefónica. Recuperado de https://www.telefonica.com/es/sala-comunicacion/blog/acuerdo-union-europea-mercosur-oportunidad-unica/

Carrillo, A. J., & Jackson, M. (2022). Follow the leader? A comparative law study of the EU's general data protection regulation's impact in Latin America. ICL Journal, 16(2), 177-262. https://doi.org/10.1515/icl-2021-0037

Chavarría-Mora, E. (2025). (Lack of) patterns in commitment: Data protection in the Latin America and Caribbean Personal data protection

laws. Social Media + Society, 11(2), 1-13. https://doi.org/10.1177/20563051251337206

European Data Protection Board. (2020). Guidelines 04/2020 on Data Protection by Design and by Default. Version 1.1, 18 November 2020.

Data Protection: 80% of National Authorities Underfunded, EU bodies “Unable to Fulfil Legal Duties” (2022, 30 September). Statewatch. https://www.statewatch.org/news/2022/september/data-protection-80-of-national-authorities-underfunded-eu-bodies-unable-to-fulfil-legal-duties

Data Protection Laws of the World https://www.dlapiperdataprotection.com/

Edler, J., Blind, K., Kroll, H., & Schubert, T. (2023). Technology sovereignty as an emerging frame for innovation policy: Defining rationales, ends and means. Research Policy, 52(6), Article 104765. https://doi.org/10.1016/j.respol.2023.104765

Felzmann, H., Villaronga, E. F., Lutz, C., & Tamò-Larrieux, A. (2019). Transparency you can trust: Transparency requirements for artificial intelligence between legal norms and contextual concerns. Big Data & Society, 6(1), 1-14. https://doi.org/10.1177/2053951719860542

Forbrukerrådet (2018). Deceived by design. Norwegian Consumer Council (Forbrukerrådet) Report, 27 June 2018. https://storage02.forbrukerradet.no/media/2018/06/2018-06-27-deceived-by-design-final.pdf

Giay, G. P., Fernández, D., & Adrogué, M. (2021, April 27). Nuevo Acuerdo de Comercio Electrónico del Mercosur. Marval O'Farrell Mairal. https://www.marval.com/publicacion/nuevo-acuerdo-de-comercio-electronico-del-mercosur-13969?lang=es

Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. L. (2018, April). The dark (patterns) side of UX design. In Proceedings of the 2018 CHI conference on human factors in computing systems (pp. 1-14).

Grisales Rendón, L. (2022). Latin American eGovernance and data protection: the EU model. In Proceedings of the Central and Eastern European eDem and eGov Days (pp. 100-105).

GSMA. (2017, September). Cross-Border Data Flows Enable the Digital Economy [4-page Spanish brochure]. Retrieved June 20, 2025, from https://www.gsma.com/…/GSMA-Cross-Border-Data-Flows-Enable-the-Digital-Economy_4pp_SPANISH_WEB.pdf

Guadamuz A (2001). Habeas Data vs the European Data Protection Directive. The Journal of Information, Law and Technology (JILT) (3). ttp://elj.warwick.ac.uk/jilt/01-3/guadamuz.html

Guio, A. (2024). Regulatory sandboxes and artificial intelligence in Latin America and Europe.

Hilton, M. (2023, September). Dark patterns and user mental health: Identifying theoretical impacts of deceptive design on vulnerable demographics. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting (pp. 2124-2127). SAGE.

Hummel, P., Braun, M., Tretter, M. & Dabrock, P. (2021). Data Sovereignty: A Review. Big Data & Society, 8 (1), 1-17. https://doi.org/10.1177/2053951720982

Jelinek, A. & Wiewiórowski, W. (2022, September 12) [Open letter]. https://www.edps.europa.eu/system/files/2022-09/22-09-12_edps-edpb-open-letter-budget-2022_en.pdf

Hutchinson, J., Stilinovic, M. & Gray, J. E. (2024). Data Sovereignty: The Next Frontier for Internet Policy? Policy & Internet, 16(1), 6-11. https://doi.org/10.1002/poi3.386

InCountry. (2025, March 6). The EU's Data Sovereignty Framework. https://incountry.com/blog/the-eus-data-sovereignty-framework/

Lee, J. D., & See, K. A. (2004). Trust in automation: Designing for appropriate reliance. Human Factors, 46(1), 50-80.

Lehuedé, H. (2019). Corporate governance and data protection in Latin America and the Caribbean. Production Development series, No. 223 (LC/TS.2019/38), Santiago, Economic Commission for Latin America and the Caribbean (ECLAC)

Luguri, J., & Strahilevitz, L. J. (2021). Shining a light on dark patterns. Journal of Legal Analysis, 13(1), 43-109.

Mejias, Ulises. (2023). Sovereignty and Its Outsiders. Weizenbaum Journal of the Digital Society, 3(2), 1-9. https://doi.org/10.34669/wi.wjds/3.2.7

Passi, S., & Vorvoreanu, M. (2022). Overreliance on AI literature review. Microsoft Research, 339, 340.

Red Iberoamericana de Protección de Datos. (2021). Guía iberoamericana para la implementación de cláusulas contractuales modelo (SCC). Recuperado de https://www.redipd.org/sites/default/files/2021-11/red-iberoamericana-guia-implementacion-scc-2021.pdf

Ringe, W.-G. (2023). AI Regulation and the Role of Regulatory Sandboxes in Europe.

Sombra, T. L. (2020). The General Data Protection Law in Brazil: What Comes Next? Global Privacy Law Review, 1(2).

Special Eurobarometer 487a (2019). The General Data Protection Regulation. European Commission, March 2019. https://cnpd.public.lu/content/dam/cnpd/fr/actualites/international/2019/ebs487a-GDPR-sum-en.pdf

Schwartz, P. (2019). Global Data Privacy: The EU Way. New York University Law Review, 94(4), 771-818. https://www.nyulawreview.org/wp-content/uploads/2019/10/NYULAWREVIEW-94-4-Schwartz.pdf

Tamò-Larrieux, A., Guitton, C., Mayer, S., & Lutz, C. (2024). Regulating for trust: Can law establish trust in artificial intelligence?. Regulation & Governance, 18(3), 780-801.

Velasco, C., & Rascovsky, M. A. (2022). Privacy and data protection law in Mexico. Wolters Kluwer.

Wagner, A. R., Borenstein, J., & Howard, A. (2018). Overtrust in the robotic age. Communications of the ACM, 61(9), 22-24.

World Bank Group. (2020). Overview of Regulatory Sandboxes in LATAM and the EU.

Zac, A., Huang, Y. C., von Moltke, A., Decker, C., & Ezrachi, A. (2023). Dark patterns and consumer vulnerability. Behavioural Public Policy, 1-50. https://doi.org/10.1017/bpp.2024.49

Voss, W. G. and Castets-Renard, C. (2016) Proposal for an International Taxonomy on the

Various Forms of the “Right to be Forgotten”: A Study on the Convergence of Norms. Colorado Technology Law Journal, 14(2), 281-344.

PROJECT INFORMATION

CALL: ERASMUS-JMO-2024-NETWORKS (Jean Monnet Policy Debate)	**TOPIC:** ERASMUS-JMO-2024-NETWORKS-HEI-NON-EU-LATIN-AMERICA
TYPE OF ACTION: ERASMUS-LS (ERASMUS Lump Sum Grants)	**PROPOSAL NUMBER:** 101176829
PROPOSAL ACRONYM: HEMISPHERES	**TYPE OF MODEL GRANT AGREEMENT:** ERASMUS Lump Sum Grant
REPORTING PERIOD: From 01.11.2024 to 31.11.2027	**TYPE OF MODEL GRANT AGREEMENT:** ERASMUS Lump Sum Grant
REPORT VERSION: 1.0	**DATE OF PREPARATION:** 26.08.2025
BENEFICIARY ORGANIZATION: Technical University of Munich (TUM), Germany	
PRINCIPAL INVESTIGATOR: Urs Gasser	**PROJECT COORDINATOR:** Pablo Gómez Ayerbe
PROJECT COORDINATOR ORGANIZATION: Technical University of Munich (TUM), Germany	**PROJECT COORDINATOR EMAIL ADDRESS:** pablo.ayerbe@tum.de