PERSPECTIVES ON DATA PROTECTION FOR THE FUTURE:

REGULATORY CONVERGENCE AND ADAPTATION

Authors:

Dandara Ramos Silvestre

Thiago Xavier Peregrino

Revisors:

Felipe Gabriades

Fernando Bousso

b/luz

b/luz

Summary

Introduction

The field of privacy and personal data protection is going through a period of tension, driven by the expansion of data-based technologies, the evolution of artificial intelligence, and the central role of digital platforms in organizing social and economic life. This context has highlighted the limits of fragmented regulatory approaches and repositioned data protection as a strategic element of digital ecosystem governance.

Across different jurisdictions, a dual trend can be observed. On one hand, there is the consolidation of regulatory convergence, with the articulation of data protection, information security, algorithmic governance, and digital accountability. On the other hand, there are intense debates on flexibility, simplification, and proportionality, especially in scenarios involving innovation and competitiveness. Data protection thus comes to be seen simultaneously as an axis of regulatory integration and as an object of adjustments aimed at adapting rules to the complexity of the digital environment.

In Brazil, this movement is clearly reflected in the expansion of the institutional role of the National Data Protection Agency (ANPD), which has been assuming broader functions of coordination and normative guidance, particularly in relation to emerging agendas such as the regulation of artificial intelligence and the protection of children and adolescents in the digital environment. In parallel, international debates, such as those related to the Digital Omnibus in the European Union, have begun to influence regulatory expectations and governance practices in the Brazilian context as well.

1. Regulatory convergence as a trend

Regulation of the digital environment has evolved from the recognition that its challenges cannot be addressed in a compartmentalized manner. In the context of intensive data circulation and growing technological complexity, isolated regulatory approaches have proven insufficient, requiring integrated perspectives that take into account the interdependence between technologies, business models, and legal risks.

In this context, regulators have begun to acknowledge the progressive blurring of boundaries between privacy, competition law, consumer protection, and cybersecurity, encouraging coordination among authorities to address risks that cut across multiple regulatory domains. Personal data protection thus ceases to occupy a restricted normative space and begins to engage directly with other core areas of the digital ecosystem.

Regulatory fragmentation tends to generate protection gaps, legal uncertainty, and practical compliance difficulties, especially for companies operating across multiple jurisdictions and facing a complex mosaic of sector specific obligations that, when not harmonized, result either in burdensome overlaps or in unintended regulatory loopholes.

These challenges become even more evident in the face of transversal and often cross border technologies such as artificial intelligence, big data, the internet of things, and digital platforms. Artificial intelligence systems, in particular, typically rely on large scale and combined data processing, increasing risks related to the legal basis of processing activities, the definition of purposes, transparency, and undesirable situations of algorithmic discrimination.

Regulatory harmonization therefore emerges as a tool for risk mitigation and the promotion of legal certainty, by aligning minimum protection principles and reducing normative conflicts. This convergence is also reflected in the growing proximity between data protection and other branches of law, such as competition law and information security, illustrating the increasing entanglement of risks and impacts already observed in regulatory initiatives and concrete cases.

> **AROUND THE WORLD**
>
> In the context of the European Union, cross cutting regulatory action is reflected in initiatives such as the Digital Markets Act (DMA)[1], which aims to foster competitiveness in the region's digital market and, to that end, establishes rules on data sharing between platforms and on guaranteeing users' freedom of choice[2], and the Digital Services Act (DSA)[3], which seeks to integrate data protection authorities and consumer protection bodies into joint supervisory mechanisms. These instruments illustrate the incorporation of privacy and data protection concerns into regulatory regimes traditionally focused on competition.

1 EUROPEAN UNION. **Regulation (EU) 2022/1925** of the European Parliament and of the Council, of 14 September 2022, on contestable and fair markets in the digital sector (Digital Markets Act – DMA). Official Journal of the European Union, Brussels, 2022. Available at: https://eur-lex.europa.eu/eli/reg/2022/1925/oj/eng. Accessed in: January 22, 2026.

2 EUROPEAN COMMISSION. **Commission sends preliminary findings to Meta over its "Pay or Consent" advertising model for non-compliance with the DMA**. Web, 2024. Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_24_3582. Accessed in: January 22, 2026.

3 EUROPEAN UNION. **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). Official Journal of the European Union, Brussels, 2022. Available at: https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng. Accessed in: January 22, 2026.

Still within the European framework, this logic is also expressed through coordination among supervisory authorities and alignment with cybersecurity and digital resilience frameworks, such as NIS2[4] and DORA[5], which were designed to operate in a way that avoids overlapping sanctions[6].

In Brazil, a similar dynamic emerged in 2021, when the Administrative Council for Economic Defense (CADE), the National Consumer Secretariat (Senacon), the Federal Public Prosecutor's Office, and the ANPD acted jointly in the analysis of data processing practices by private entities[7]. This movement was institutionalized through cooperation agreements between CADE and the ANPD[8], and later with Senacon, as well as through the creation of the National Consumer Defense Council (CNDC)[9], reinforcing convergence among competition law, data protection, and the protection of consumer rights.

Regulatory convergence, therefore, is not limited to the harmonization of data protection rules but rather points toward the construction of an integrated regulatory paradigm aimed at the governance of the digital ecosystem as a whole. It is within this context that the relevance of authorities capable of acting as connecting points between distinct legal regimes is strengthened, a role that has been progressively shaped for the ANPD throughout 2025, with expectations of further consolidation in the coming years.

4 EUROPEAN UNION. **Directive (EU) 2022/2555** of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Official Journal of the European Union, Brussels, 2022. Available at: https://eur-lex.europa.eu/eli/dir/2022/2555/oj. Accessed in: January 22, 2026.

5 EUROPEAN UNION. **Regulation (EU) 2022/2554** of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011. Official Journal of the European Union, Brussels, 2022. Available at: https://eur-lex.europa.eu/eli/reg/2022/2554/oj. Accessed in: January 22, 2026.

6 EUROPEAN COMMISSION. **Digital Operational Resilience Act (DORA): Factsheet**. Web, s/d. Available at: https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en. Accessed in: January 22, 2026.

7 BRAZIL. Administrative Council of Economic Defense. **Cade, MPF, ANPD e Senacon recomendam que WhatsApp adie entrada em vigor da nova política de privacidade**. Web, 2021. Available at: https://www.gov.br/anpd/pt-br/assuntos/noticias/cade-mpf-anpd-e-senacon-recomendam-que-whatsapp-adie-entrada-em-vigor-da-nova-politica-de-privacidade. Accessed in: January 22, 2026.

8 BRAZIL. National Data Protection Agency. **Acordo de Cooperação Técnica nº 5/2021**. Firma cooperação entre a ANPD e o CADE. Official Gazette of the Union, Brasília, DF, 2021. Available at: https://www.gov.br/anpd/pt-br/acesso-a-informacao/convenios-e-transferencias/documentos/act-cade_ocultado.pdf. Accessed in: January 22, 2026.

9 BRAZIL. **Decreto nº 10.417, de 7 de julho de 2020**. Institui o Conselho Nacional de Defesa do Consumidor. Official Gazette of the Union, Brasília, DF, 2020. Available at: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10417.htm. Accessed in: January 22, 2026.

2. The expansion of the institutional role of the National Data Protection Agency

The ANPD has undergone an accelerated process of institutional development since its creation, progressively consolidating itself as one of the main actors in the Brazilian digital regulatory ecosystem. Initially conceived to oversee compliance with the LGPD, the Agency has, over recent years, assumed responsibilities that go beyond the strict application of this legal framework, significantly expanding the scope of its activities and reinforcing its position as a strategic body for regulatory coordination.

A first milestone in this process occurred in 2022, when the ANPD was transformed from a federal public administration body linked to the Office of the President into a special purpose autonomous entity[10], thereby gaining greater administrative and financial autonomy. This change laid the groundwork for a more stable regulatory action, less dependent on circumstantial arrangements and more aligned with the complexity of the risks associated with data processing in the digital environment.

This process of institutional strengthening reached a new level in September 2025, when the ANPD was elevated to the status of an independent regulatory agency through Provisional Measure No. 1,317 of 2025[11]. The formal transformation into a regulatory agency, with inclusion in the regulatory agencies framework and reinforcement of its functional, technical, decision making, administrative, and financial autonomy, represents a significant departure from the previous institutional design and expands the Agency's capacity to influence public policies in the country in a continuous and structural manner.

From a substantive perspective, this new status qualitatively alters the way the ANPD operates. Decision making autonomy strengthens the effectiveness of its supervisory and sanctioning powers, allowing the initiation of administrative proceedings and the imposition of penalties with greater independence. At the same time, institutional reinforcement expands the Agency's operational capacity, including through the enlargement of its specialized technical staff, which is essential to address complex demands related to auditing, inspections, and the analysis of risks associated with new technologies. Added to this is the strengthening of its technical normative authority, which consolidates the ANPD as the central body for interpreting the LGPD and for issuing guidelines capable of orienting both the public and private sectors in the face of innovative business models.

This institutional evolution takes place in a context in which personal data has become essential infrastructure for emerging technologies and for platform based economic dynamics. As a result, the ANPD tends to move from a predominantly reactive role, centered on ex post supervision, toward broader functions of coordination, normative guidance, and interinstitutional articulation.

10 BRAZIL. **Lei nº 14.460, de 25 de outubro de 2022.** Transforma a Autoridade Nacional de Proteção de Dados (ANPD) em autarquia de natureza especial e transforma cargos comissionados. Official Gazette of the Union, Brasília, DF, 2022. Available at: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/lei/l14460.htm. Accessed in: January 22, 2026.

11 BRAZIL. **Medida Provisória Nº 1.317, de 17 de setembro de 2025**. Altera a Lei nº 13.709, de 14 de agosto de 2018, para tratar da Agência Nacional de Proteção de Dados, a Lei nº 10.871, de 20 de maio de 2004, para criar a Carreira de Regulação e Fiscalização de Proteção de Dados, transforma cargos no âmbito do Poder Executivo federal, e dá outras providências. Official Gazette of the Union, Brasília, DF, 2025. Available at: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2025/Mpv/mpv1317.htm. Accessed in: January 22, 2026.

This shift is consistent with the previously described trend of regulatory convergence. The more digital risks overlap, the more relevant it becomes to have an authority capable of operating as an integrating axis of related agendas.

In this sense, the expansion of ANPD's role is also reflected in the broadening of its substantive competences. Two particularly relevant axes stand out in this context: the protection of children and adolescents in the digital environment and the regulation of artificial intelligence. Both illustrate how personal data protection comes to function as an organizing foundation for broader regulatory responses aimed at safeguarding fundamental rights in complex digital ecosystems.

Concerning the protection of children and adolescents, the Digital Statute of the Child and Adolescent (Digital ECA) assigns the ANPD with supervisory powers related to the processing of data of this population, positioning the Agency as an administrative guardian of enhanced duties of protection, security measures, and governance practices appropriate to minors. This movement expands the scope of data protection beyond a general compliance logic, bringing it closer to the protection of vulnerable groups.

In parallel, the growing centrality of artificial intelligence in the digital economy has driven the consolidation of the ANPD as a key player in the governance of these technologies.

2.1. ANPD's role in the artificial intelligence regulatory framework

In the context of the text currently under discussion of Bill No. 2,338 of 2023[12], which establishes the regulatory framework for artificial intelligence in Brazil, the ANPD assumes a central role in the institutional architecture of AI governance. The version approved by the Federal Senate and currently under consideration by the Chamber of Deputies consolidates the ANPD as one of the main bodies responsible for the regulation, supervision, and coordination of the use of artificial intelligence systems.

The bill assigns the ANPD the function of residual regulator, granting it normative, supervisory, and sanctioning powers to regulate AI systems used in sectors that do not have their own regulatory agency. Under this model, sectoral authorities remain responsible for regulating AI applications within their respective domains, such as health, finance, or telecommunications, while the ANPD acts in a supplementary manner in sectors lacking specific regulation. The objective is to avoid regulatory gaps and to ensure a minimum standard of legal protection in the use of artificial intelligence, regardless of the economic sector involved.

In addition, the Bill positions the ANPD as the coordinating authority of the National System for the Regulation and Governance of Artificial Intelligence (SIA). In this capacity, the Agency will be responsible for articulating the actions of the various regulatory entities that make up the system, promoting normative harmony, institutional cooperation, and coherence in supervisory

12 BRAZIL. Chamber of Deputies. **Projeto de Lei nº 2.338/2023**. Dispõe sobre o desenvolvimento, o fomento e o uso ético e responsável da inteligência artificial com base na centralidade da pessoa humana. Chamber of Deputies, Brasília, DF, 2023. Available at: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2868197&filename=PL%202338/2023. Accessed in: January 22, 2026.

actions related to the topic. The ANPD will also play a central role in the Permanent Council for Regulatory Cooperation in Artificial Intelligence, a body created to foster interinstitutional dialogue and coordinated state action in the governance of this type of technology.

The centrality of the ANPD within this regulatory framework stems largely from its institutional vocation for the protection of personal data and privacy, dimensions closely linked to the functioning of artificial intelligence systems. The Bill itself emphasizes that the competences attributed to the Agency do not replace, but rather complement, those already provided for under the LGPD. In this sense, the ANPD comes to play a strategic role in ensuring that the development, implementation, and use of AI systems observe principles such as purpose limitation, necessity, transparency, non-discrimination, and accountability, especially when they involve automated processing of personal data.

The Bill assigns the ANPD the responsibility of monitoring and supervising the risks associated with the use of artificial intelligence, with particular attention to impacts on personal data and the rights of data subjects. The proposed model provides for coordinated action by the ANPD with other bodies within the SIA in joint investigations, including for the determination of violations and the application of sanctions, especially in cases involving systems classified as high-risk.

Another relevant axis concerns the normative competence granted to the Agency. The Bill establishes that the ANPD will be responsible for issuing general rules, guidance, and technical guidelines on AI governance, particularly regarding automated processing of personal data, algorithmic transparency, impact assessments, and communication of relevant incidents. These general rules are intended to serve as a basis for specific sectoral regulations, reinforcing the ANPD's function as a structural component of the regulatory system.

From a legislative perspective, although the Bill is still in the final stages of discussion in the Chamber of Deputies, with the possibility of adjustments to the governance model and to the definition of the ANPD's competences, the institutional design proposed and debated already points to the consolidation of the Agency as a central figure in the regulation of artificial intelligence in Brazil.

DIRECT IMPACTS ON THE ACTIVITIES OF THE ANPD

The topic of artificial intelligence has become a consistent component of the ANPD's Regulatory Agenda, particularly during the 2023 and 2024 biennium, when the topic was included as a specific axis of action, a position that is maintained in the Regulatory Agenda proposed for the 2025 to 2026 biennium[13]. In this context, the Agency conducted studies, public consultations, and calls for contributions focused on the review of automated decisions and the use of AI under the framework of the LGPD, signaling an intention to regulate Article 20[14] of the LGPD in greater detail.

The continuity of this movement is also evident in the ANPD's Priority Topics Map, which has expressly included artificial intelligence and emerging technologies as priority areas for

13 BRAZIL. National Data Protection Agency. **Resolução CD/ANPD nº 31, de 22 de dezembro de 2025.** Altera a Agenda Regulatória para o biênio 2025-2026. Official Gazette of the Union, Brasília, DF, 2025. Available at: https://www.in.gov.br/web/dou/-/resolucao-cd/anpd-n-31-de-22-de-dezembro-de-2025-677950080. Accessed in: January 22, 2026.

14 Article 20. The data subject is entitled to request the review of decisions made solely based on automated processing of personal data that affect his/her interests, including decisions intended to define his/her personal, professional, consumer and credit profile or aspects of his/her personality.

> enforcement in the years 2026 and 2027[15]. This orientation highlights the Agency's concern with risks such as excessive profiling, algorithmic discrimination, decision making opacity, and the use of automated systems in sensitive contexts, both in the private sector and in the public sector.

The role of the ANPD tends to be affirmed as a key element in ensuring that the progression of artificial intelligence occurs in a responsible, ethical, and legally sound manner, reconciling economic development, innovation, and the protection of fundamental rights. The Agency thus comes to occupy a strategic position not only as the regulator of personal data use, but also as one of the main pillars of artificial intelligence governance within the Brazilian legal system.

2.2. The role of the ANPD under the Digital ECA and the protection of children and adolescents in the online environment

Another central vector in the expansion of the ANPD's substantive competences concerns the protection of children and adolescents in the digital environment. The enactment of the Digital ECA represents a relevant milestone in this process by assigning the ANPD an explicit institutional role in supervising the processing of personal data of this population in digital contexts.

The attribution of these competences to the ANPD does not occur in isolation, but rather forms part of the same regulatory convergence movement observed in the governance of artificial intelligence. From the Agency's perspective, and in line with the Brazilian tradition of protecting minors, children and adolescents constitute a particularly vulnerable group in digital ecosystems marked by intensive data collection, profiling techniques, behavioral advertising, and algorithmic systems of recommendation and engagement. In this scenario, data protection comes to function as a vector for the safeguarding of fundamental rights, connecting privacy, security, healthy development, and protection against abusive practices.

The Digital ECA consolidates the ANPD as the autonomous administrative authority responsible for supervising the processing of data of children and adolescents, including with respect to age verification, the obtaining of parental consent when applicable, the adoption of appropriate security measures, and the implementation of preventive mechanisms in digital platforms and services aimed at or accessible to children and adolescents. By assuming this role, the ANPD expands its original mandate under the LGPD and begins to act also as a guardian of the rights of a vulnerable group in the online environment.

From a regulatory perspective, the Digital ECA also strengthens the exercise of the ANPD's technical normative power. The Agency acquires competence to issue specific guidance on best practices for the processing of children's and adolescents' data, directly influencing the design of digital products, data-driven business models, and the compliance strategies of digital platforms. This represents a significant shift. Data protection ceases to operate merely

15 BRAZIL. National Data Protection Agency. **Resolução CD/ANPD nº 30, de 23 de dezembro de 2025.** Aprova o Mapa de Temas Prioritários para o biênio 2026-2027. Official Gazette of the Union, Brasília, DF, 2025. Available at: https://www.in.gov.br/web/dou/-/resolucao-cd/anpd-n-30-de-23-de-dezembro-de-2025-677947163. Accessed in: January 22, 2026.

as a transversal obligation and increasingly conditions the very architecture of digital services targeted at sensitive audiences, in line with the Privacy by Design methodology.

As in the field of artificial intelligence, the ANPD's role under the Digital ECA reflects a qualitative change in its institutional function. The Agency does not act only as an enforcer of already established conduct, but as a structuring agent of preventive governance, oriented toward risk mitigation from the conception of digital systems and services. In this sense, even though the obligations of the Digital ECA will only enter into force in March 2026, the Agency has already initiated prior monitoring actions in relation to several companies affected by the law's entry into force, with the purpose of assessing their level of legal maturity and strategic planning for ongoing compliance with the new regulation[16].

This movement reinforces the understanding that data protection, especially when involving children and adolescents, constitutes a central element of the regulation of the contemporary digital ecosystem.

AROUND THE WORLD

The Brazilian choice to assign to a data protection authority the competence to oversee the protection of children and adolescents in the digital environment stands out in comparison with other jurisdictions.

When comparing Brazilian legislation with the United Kingdom's Online Safety Act[17], an international framework that influenced the adoption of the Digital ECA, it becomes clear that the responsibilities attributed to the ANPD in Brazil are, in the UK context, assigned to the Office of Communications (Ofcom), an independent regulatory body responsible for telecommunications, radio, television, and the internet. Even so, this does not preclude, in specific contexts, the need for cooperation between Ofcom and the UK data protection authority, the Information Commissioner's Office (ICO)[18].

16 BRAZIL. National Data Protection Agency. **Em ação de monitoramento do ECA Digital, a ANPD estende o prazo para que empresas prestem informações sobre implementação das novas regras.** Web, 2026. Available at: https://www.gov.br/anpd/pt-br/assuntos/noticias/em-acao-de-monitoramento-do-eca-digital-a-anpd-estende-o-prazo-para-que-empresas-prestem-informacoes-sobre-implementacao-das-novas-regras. Accessed in: January 20, 2026.

17 UNITED KINGDOM. **Online Safety Act 2023 Chapter 50.** An Act to make provision for and in connection with the regulation by OFCOM of certain internet services; for and in connection with communications offences; and for connected purposes. The Stationery Office, London, 2023. Available at: https://www.legislation.gov.uk/ukpga/2023/50. Accessed in: January 22, 2026.

18 OFCOM. **Ofcom and the Information Commissioner's Office (ICO) have published a joint statement on collaboration on the regulation of online services.** Web, 2024. Available at: https://www.ofcom.org.uk/online-safety/safety-technology/online-safety-and-data-protection. Accessed in: January 22, 2026.

3. Digital Omnibus and the reflexes of the European debate in Brazil

The recent expansion of the ANPD's areas of action cannot be explained solely by internal governance adjustments and institutional strengthening. It is also increasingly connected to a global regulatory environment undergoing rapid transformation. On one hand, Brazil is witnessing an expansion of ANPD's supervisory scope in the digital environment. On the other, there is the consolidation of a new European regulatory cycle that is broader, more transversal, and strategically oriented toward the unification of its digital regulatory ecosystem, with effects that tend to radiate beyond the European Union and influence corporate practices and legislative debates elsewhere. It is within this second axis that the package proposed under the Digital Omnibus is situated, whose analysis is particularly relevant for understanding the future of the Brazilian regulatory debate.

The Digital Omnibus was presented by the European Commission as a package aimed at simplifying and adjusting the implementation of core digital regulations, with the objective of reducing frictions, overlaps, and practical uncertainties. Broadly speaking, the package is composed of two distinct regulatory proposals: one has a broad digital focus[19], introducing technical amendments and adjustments across multiple components of the European digital framework; and the other focuses on artificial intelligence[20], with changes specifically targeted at the implementation and enforcement regime of the EU AI Act[21]. The package engages with adjacent issues of privacy and digital compliance, reflecting the European perception that the accumulated complexity of the regulatory framework, if not properly addressed, may undermine both its effectiveness and the EU's competitiveness.

For Brazil, the central issue is not the literal importation of these solutions, but rather the way in which they project themselves through what is known as the "Brussels Effect", that is, the European Union's capacity to export its regulatory standards, directly or indirectly. This potential exportation may occur through two main channels.

The first is economic and operational. Global companies tend to unify their compliance and governance practices based on the European standard in order to avoid fragmentation and segmentation costs, especially when operating across multiple jurisdictions.

19 EUROPEAN UNION. European Commission. **Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus).** European Commission, Brussels, 2025. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025PC0837. Accessed in: January 22, 2026.

20 EUROPEAN UNION. European Commission. **Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI).** European Commission, Brussels, 2025. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025PC0836. Accessed at: January 22, 2026.

21 EUROPEAN UNION. **Regulation (EU) 2024/1689** of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). Official Journal of the European Union, Brussels, 2024. Available at: http://data.europa.eu/eli/reg/2024/1689/oj. Accessed in: January 22, 2026.

The second is normative and political. European legislation and guidance function as reference points for local reforms, influencing both legal language and the institutional architecture of public policies in third countries. This was the case with the GDPR, whose impact extended beyond European borders, and there are consistent signs that the same logic is now being reinforced with the EU AI Act and with the broader set of instruments surrounding European digital regulation.

REGULATORY IMPACTS

1. **Enforcement design and institutional governance.**

The European emphasis on coordination and consistent supervision, including greater centralization of competences within specialized structures, tends to fuel debates in Brazil on the institutional design of enforcement, integration among sectoral authorities, and the residual role of cross cutting authorities, especially in the context of discussions on new legal frameworks.

2. **Rationalization of compliance as a regulatory agenda.**

The Digital Omnibus is based on a diagnosis of accumulated complexity and seeks, at least in theory, to reduce implementation frictions. This type of agenda tends to resonate in Brazil, particularly in regulated sectors and in the field of digital governance, where pressure for simplification coexists with demands for regulatory effectiveness.

3. **Pressure for convergence and regulatory benchmarking.**

Even if Brazil does not replicate the European solution, the European debate frequently functions as a benchmark for legislators, regulators, and courts, influencing risk language, expectations of accountability, and the definition of minimum duties. There is a sensitive point here. If the Digital Omnibus is perceived by some actors as excessive flexibility, it may trigger reactions in the opposite direction, with local tightening. If it is seen as a pragmatic adjustment, it may legitimize more gradual and risk-based approaches.

In summary, the Digital Omnibus should be read as part of the maturation process of the European model. It is not simply a move toward less regulation, but rather an attempt to reorganize compliance costs and implementation timelines without, at least formally, abandoning the risk-based protection structure.

For Brazil, the main effect is indirect but significant. It reshapes the reference environment for public policies and corporate programs, reframing the debate on how to regulate artificial intelligence and data without undermining innovation. This tension may become one of the central drivers of the next phase of digital regulation.

4. Final considerations: the future of data protection in Brazil

Recent transformations in the field of privacy and personal data protection indicate that the regulatory debate has entered a new phase, marked less by the creation of isolated regimes and more by the pursuit of systemic coherence, institutional coordination, and the adaptation of rules to the complexity of the digital environment. Regulatory convergence emerges, in this context, not as a methodological choice, but as a necessary response to the interdependence between technologies, business models, and legal risks that cut across multiple regulatory domains.

In Brazil, this movement materializes particularly clearly in the expansion of the institutional role of the ANPD. The Agency moves beyond a role limited to enforcing the LGPD and consolidates itself as a central authority within the digital regulatory ecosystem, with functions that combine enforcement, normative guidance, and interinstitutional coordination.

The incorporation of new substantive fronts, such as artificial intelligence governance and the protection of children and adolescents in the digital environment, highlights a qualitative shift in the ANPD. Data protection comes to operate as a structuring axis for broader regulatory responses aimed at safeguarding fundamental rights in complex technological contexts.

At the same time, the European debate surrounding the Digital Omnibus shows that the growth of regulatory regimes also involves reflections on proportionality, regulatory timing, and the rationalization of compliance costs. Far from representing a simple regulatory retreat, these initiatives signal an effort to adjust regulatory instruments in order to make them more effective, without abandoning a risk-based protection logic.

In this scenario, future perspectives for data protection in Brazil tend toward a model that is less centered on formal compliance and more oriented toward governance, accountability, and integration among legal regimes. For companies, this implies the need for more sophisticated compliance structures capable of engaging simultaneously with privacy, information security, algorithmic governance, and the protection of vulnerable groups.

For regulators, the challenge will be to balance the expansion of competences, interinstitutional coordination, and regulatory predictability, avoiding both fragmentation and excessive normative complexity.

b/luz

www.baptistaluz.com.br/