



LUCA BELLÌ, ANA BRIAN,
ARMANDO MANZUETA, NICOLO ZINGALES

DA AUTODETERMINAÇÃO INFORMATIVA À SOBERANIA DOS DADOS

UM FRAMEWORK DE GOVERNANÇA

FROM INFORMATIONAL SELF- DETERMINATION TO DATA SOVEREIGNTY

A GOVERNANCE FRAMEWORK

From Informational Self-Determination to Data Sovereignty

Da Autodeterminação Informativa à Soberania dos Dados: Um Framework de Governança

Luca Belli, Ana Brian, Armando Manzueta, Nicolo Zingales

ARTIGO PARA DISCUSSÃO APRESENTADO NA **COMPUTERS, PRIVACY AND DATA PROTECTION CONFERENCE LATIN AMERICA (CPDP LATAM) 2026**. ENVIE COMENTÁRIOS ATÉ **30 DE AGOSTO** PARA CTS@FGV.BR.

DISCUSSION PAPER PRESENTED AT THE **COMPUTERS, PRIVACY AND DATA PROTECTION CONFERENCE LATIN AMERICA (CPDP LATAM) 2026**. SEND COMMENTS UNTIL **AUGUST 30** TO CTS@FGV.BR.

DISCUSSION PAPER PRESENTADO EN LA **COMPUTERS, PRIVACY AND DATA PROTECTION CONFERENCE LATIN AMERICA (CPDP LATAM)**. ENVIAR COMENTARIOS HASTA EL **30 DE AGOSTO** PARA CTS@FGV.BR.

Abstract

Data has become one of the defining strategic resources of the twenty-first century. It fuels artificial intelligence, supports digital public services, enables innovation, facilitates international trade, and increasingly determines geopolitical influence. However, despite the multiple facets of data governance, regulatory responses have primarily focused on establishing legal guarantees for the protection of personal data. This paper contends that, while these guarantees remain indispensable for safeguarding individual rights and democratic values, they have proven insufficient to address the broader structural challenges arising from the concentration of digital infrastructures, technological dependence, cybersecurity risks and the unequal distribution of value within the global data economy.

Indeed, the infrastructures through which data are generated, processed, stored and exchanged remain highly concentrated among a limited number of private corporations and jurisdictions. This concentration has generated unprecedented economic dependencies, cybersecurity vulnerabilities, and governance

asymmetries, placing the concept of data sovereignty at the center of contemporary policy debates. However, despite its growing importance, data sovereignty remains an elusive concept. Existing literature often equates it with territorial control over data or with data localization requirements, while others interpret it exclusively through the lens of privacy and data protection.

This paper argues that these approaches are incomplete. Based on previous research, it argues that “data sovereignty should instead be understood as the capacity of individuals, societies and states to understand how data processing technologies work, develop alternatives and regulate them effectively, thus achieving informational self-determination and fair redistribution of value, in accordance with democratically determined objectives.” Achieving this capacity requires moving beyond the traditional doctrine of informational self-determination and embracing a multidimensional framework that integrates constitutional rights, cybersecurity, technological infrastructures, industrial development, competition policy, and fiscal justice.

The paper develops this argument in four stages. It first traces the historical evolution of informational self-determination, from its origins in German constitutional jurisprudence to its subsequent development in European, Inter-American, Asian and African legal and political traditions. It then argues that the contemporary digital economy has fundamentally transformed the conditions under which informational self-determination is exercised, requiring an expanded conception of the concept, thus evolving into data sovereignty, capable of addressing technological dependence, market concentration, and geopolitical fragmentation. The paper subsequently proposes six interdependent dimensions of data sovereignty – namely i) data protection, ii) cybersecurity, iii) Digital Public Infrastructure (DPI), iv) industrial policy, v) competition and innovation, vi) and taxation for data equity – and finally examines which type of governance framework may provide the practical foundations for building sovereign yet interconnected digital ecosystems.

Importantly, the paper argues that data sovereignty should not be equated to digital isolationism or technological autarky. On the contrary, genuine data sovereignty emerges from the capacity to participate in digital ecosystems on the basis of shared rules, being able to freely pursue one’s constitutional objectives, within a trustworthy and secure environment.

Resumo executivo

Os dados tornaram-se um dos recursos estratégicos definidores do século XXI. Eles alimentam a inteligência artificial, apoiam os serviços públicos digitais, permitem a inovação, facilitam o comércio internacional e determinam, cada vez mais, a influência geopolítica. No entanto, apesar das múltiplas facetas da governança de dados, as respostas regulatórias têm se concentrado principalmente no

estabelecimento de garantias legais para a proteção de dados pessoais. Este artigo argumenta que, embora essas garantias continuem indispensáveis para salvaguardar os direitos individuais e os valores democráticos, elas se mostraram insuficientes para abordar os desafios estruturais mais amplos decorrentes da concentração de infraestruturas digitais, da dependência tecnológica, dos riscos de segurança cibernética e da distribuição desigual de valor na economia global de dados.

De fato, as infraestruturas por meio das quais os dados são gerados, processados, armazenados e trocados permanecem altamente concentradas em um número limitado de empresas privadas e de jurisdições. Essa concentração gerou dependências econômicas sem precedentes, vulnerabilidades de cibersegurança e assimetrias de governança, colocando o conceito de soberania de dados no centro dos debates políticos contemporâneos. No entanto, apesar de sua crescente importância, a soberania de dados continua sendo um conceito difícil de definir. A literatura existente frequentemente equipara a soberania de dados ao controle territorial sobre os dados ou aos requisitos de localização de dados, enquanto outros a interpretam exclusivamente sob a ótica da privacidade e da proteção de dados.

Este artigo argumenta que essas abordagens são incompletas. Com base em pesquisas anteriores, defende que “a soberania de dados deve ser entendida como a capacidade de indivíduos, sociedades e Estados de compreender como as tecnologias de processamento de dados funcionam, desenvolver alternativas e regulá-las de forma eficaz, alcançando assim a autodeterminação informativa e a redistribuição justa de valor, de acordo com objetivos democraticamente determinados”. Alcançar essa capacidade exige ir além da doutrina tradicional da autodeterminação informativa e adotar uma estrutura multidimensional que integre direitos constitucionais, segurança cibernética, infraestruturas tecnológicas, desenvolvimento industrial, política de concorrência e justiça fiscal.

O artigo desenvolve esse argumento em quatro etapas. Primeiro, traça a evolução histórica da autodeterminação informativa, desde suas origens na jurisprudência constitucional alemã até seu desenvolvimento subsequente nas tradições jurídicas e políticas europeias, interamericanas, asiáticas e africanas. Em seguida, argumenta que a economia digital contemporânea transformou fundamentalmente as condições sob as quais a autodeterminação informativa é exercida, exigindo uma concepção ampliada do conceito, evoluindo assim para a soberania de dados, capaz de lidar com a dependência tecnológica, a concentração de mercado e a fragmentação geopolítica. O artigo propõe, então, seis dimensões interdependentes da soberania de dados – a saber: i) proteção de dados, ii) cibersegurança, iii) Infraestrutura Pública Digital (IPD), iv) política industrial, v) concorrência e inovação, vi) e tributação para a equidade de dados – e, finalmente, examina qual tipo de estrutura de governança pode fornecer as bases práticas para a construção de ecossistemas digitais soberanos, porém interconectados.

É importante ressaltar que o artigo argumenta que a soberania de dados não deve ser equiparada ao isolacionismo digital ou autarquia tecnológica. Pelo contrário, a verdadeira soberania de dados emerge da capacidade de participar em ecossistemas digitais com base em regras compartilhadas, podendo buscar livremente os seus objetivos constitucionais, dentro de um ambiente confiável e seguro.

Summary

<u>EXECUTIVE ABSTRACT.....</u>	<u>ERROR! BOOKMARK NOT DEFINED.</u>
<u>INTRODUCTION: UNRAVELING DATA SOVEREIGNTY.....</u>	<u>9</u>
<u>UPGRADING INFORMATIONAL SELF-DETERMINATION</u>	<u>12</u>
<u>DATA SOVEREIGNTY AS A GOVERNANCE</u>	
<u>CAPABILITY</u>	
<u>13</u>	<u>.....</u>
<u>ARTICLE STRUCTURE.....</u>	<u>15</u>
<u>METHODOLOGY</u>	<u>16</u>
<u>1.FROM INFORMATIONAL SELF-DETERMINATION TO DATA SOVEREIGNTY.</u>	<u>16</u>
<u>1.1. INFORMATIONAL SELF-DETERMINATION FROM THE</u>	
<u>CONSTITUTIONAL PRINCIPLE TO THE REGULATORY MODEL.....</u>	<u>18</u>
<u>1.1.1. INFORMATIONAL SELF-DETERMINATION IN THE INTER-AMERICAN</u>	
<u>HUMAN RIGHTS SYSTEM</u>	<u>21</u>
<u>1.2. CONSIDERING ASIAN PERSPECTIVES: A COLLECTIVE APPROACH TO</u>	
<u>INFORMATIONAL SELF-DETERMINATION FOR SECURITY AND</u>	
<u>DEVELOPMENT</u>	<u>23</u>
<u>1.3. AN AFRICAN PERSPECTIVE: DATA SOVEREIGNTY AS RESISTANCE TO</u>	
<u>DIGITAL COLONIALISM.....</u>	<u>25</u>
<u>1.4. CONVERGING TRADITIONS, DIVERGENT EMPHASES.....</u>	<u>27</u>
<u>2. WHY AN EXCLUSIVELY INDIVIDUALISTIC CONCEPTION OF</u>	
<u>INFORMATIONAL SELF-DETERMINATION IS NO LONGER ENOUGH</u>	<u>28</u>
<u>3. THE CONSTITUTIVE DIMENSIONS OF DATA SOVEREIGNTY.....</u>	<u>31</u>
<u>3.1. DATA PROTECTION.....</u>	<u>33</u>
<u>3.2. CYBERSECURITY AND CYBER RESILIENCE.....</u>	<u>35</u>
<u>3.3. DIGITAL PUBLIC INFRASTRUCTURE.....</u>	<u>38</u>
<u>3.4. INDUSTRIAL DEVELOPMENT AND TECHNOLOGICAL CAPACITY</u>	<u>42</u>
<u>3.5. COMPETITION AND INNOVATION</u>	<u>45</u>
<u>3.6. FISCAL JUSTICE AND DATA EQUITY</u>	<u>49</u>
<u>3.7. DATA SOVEREIGNTY AS AN INTEGRATED GOVERNANCE</u>	
<u>FRAMEWORK.....</u>	<u>51</u>
<u>4. HOW TO BUILD DATA SOVEREIGNTY.....</u>	<u>53</u>

4.1. SOVEREIGN EQUALITY AS A FOUNDATION.....	54
4.2. INTEROPERABILITY AS AN OPERATIONAL EXPRESSION OF SOVEREIGNTY.....	56
4.3. DIGITAL PUBLIC INFRASTRUCTURE AS A SHARED ENABLER.....	60
4.4. FROM DEPENDENCY TO RESILIENT INTERDEPENDENCE.....	61
CONCLUSIONS.....	62

RESUMO EXECUTIVO.....	2
INTRODUÇÃO: DESVENDANDO A SOBERANIA DE DADOS	66
FORTALECENDO A AUTODETERMINAÇÃO INFORMATIVA.....	69
A SOBERANIA DE DADOS COMO CAPACIDADE DE GOVERNANÇA	71
ESTRUTURA DO ARTIGO.....	72
METODOLOGIA	73
1.DA AUTODETERMINAÇÃO INFORMATIVA À SOBERANIA DE DADOS ...	74
1.1. DA AUTODETERMINAÇÃO INFORMATIVA: DO PRINCÍPIO	
CONSTITUCIONAL AO MODELO REGULATÓRIO.....	76
1.1.1. A AUTODETERMINAÇÃO INFORMATIVA NO SISTEMA	
INTERAMERICANO DE DIREITOS HUMANOS.....	77
1.2. CONSIDERANDO PERSPECTIVAS ASIÁTICAS: UMA ABORDAGEM	
COLETIVA DA AUTODETERMINAÇÃO INFORMATIVA PARA A SEGURANÇA E O	
DESENVOLVIMENTO	78
1.3. UMA PERSPECTIVA AFRICANA: A SOBERANIA DE DADOS COMO	
RESISTÊNCIA AO COLONIALISMO DIGITAL.....	83
1.4. TRADIÇÕES CONVERGENTES, ÊNFASES DIVERGENTES	85
2. POR QUE UMA CONCEPÇÃO EXCLUSIVAMENTE INDIVIDUALISTA DA	
AUTODETERMINAÇÃO INFORMATIVA JÁ NÃO É SUFICIENTE.....	86
3. AS DIMENSÕES CONSTITUTIVAS DA SOBERANIA DE DADOS	90
3.1. PROTEÇÃO DE DADOS	91
3.2. CIBERSEGURANÇA E RESILIÊNCIA CIBERNÉTICA	93
3.3. INFRAESTRUTURA PÚBLICA DIGITAL.....	97
3.4. DESENVOLVIMENTO INDUSTRIAL E CAPACIDADE TECNOLÓGICA... 	101
3.5. CONCORRÊNCIA E INOVAÇÃO	105
3.6. JUSTIÇA FISCAL E EQUIDADE DE DADOS.....	109
3.7. A SOBERANIA DE DADOS COMO UM MARCO INTEGRADO DE	
GOVERNANÇA	111
4. COMO CONSTRUIR A SOBERANIA DE DADOS	113
4.1. A IGUALDADE SOBERANA COMO FUNDAMENTO	114
4.2. A INTEROPERABILIDADE COMO EXPRESSÃO OPERACIONAL DA	
SOBERANIA	117
4.3. A INFRAESTRUTURA PÚBLICA DIGITAL COMO UM ELEMENTO	

<u>FACILITADOR COMPARTILHADO</u>	<u>121</u>
<u>4.4. DA DEPENDÊNCIA À INTERDEPENDÊNCIA RESILIENTE</u>	<u>122</u>
<u>CONCLUSÕES</u>	<u>124</u>

From Informational Self-Determination to Data Sovereignty

Luca Belli, Ana Brian, Armando Manzueta, Nicolo Zingales

INTRODUÇÃO: DESVENDANDO A SOBERANIA DOS DADOS

Few concepts have gained as much prominence in digital governance over the last decade as data sovereignty, digital sovereignty and AI sovereignty.¹ Indeed, governments and other stakeholders alike increasingly invoke sovereignty-related concerns when discussing cloud computing, artificial intelligence (AI), cybersecurity, cross-border data flows, digital public infrastructure, taxation of digital platforms, or strategic technological autonomy. International organizations have similarly embraced the concept as they seek to reconcile the benefits of an open digital economy with growing concerns over security, privacy, economic concentration and geopolitical rivalry.²

¹ See for instance Couture, S., & Toupin, S. (2019). What does the notion of “sovereignty” mean when referring to the digital? *New Media & Society*, 21(10), 2305-2322 ; Floridi, L. (2020) The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. *Philos. Technol.* 33, 369–378; Belli L (2021) BRICS countries to build digital sovereignty. In: Belli, L. (Ed.). *CyberBRICS: Cybersecurity Regulations in the BRICS Countries*. Cham: Springer. pp 271–280; Belli, L. (2023). ; Kovacs, A., Ranganathan, N. (2019). *Data sovereignty, of whom? Limits and suitability of sovereignty frameworks for data in India*. Data Governance Network Working Paper 03; Luca Belli, 'Building Good Digital Sovereignty through Digital Public Infrastructures and Digital Commons in India and Brazil' (T20 India 2023); Luca Belli, 'To Get Its AI Foothold, Brazil Needs to Apply the Key AI Sovereignty Enablers (KASE)' in S Feldstein (ed), *New Digital Dilemmas: Resisting Autocrats, Navigating Geopolitics, Confronting Platforms* (Carnegie 2023); Chander, A., & Sun, H. (Eds.). (2023). *Data Sovereignty: From the Digital Silk Road to the Return of the State*. Oxford University Press; Belli, L., 'BRICS countries and AI sovereignty: Introduction to Thematic Section' (2024) 34 *AJIC* 1, 1–6; Belli, L. (2025). Exploring the Key AI Sovereignty Enablers (KASE) of Brazil, to Build an AI Sovereignty Stack. In: Belli, L. and Gaspar W.B. (eds), *The Quest for AI Sovereignty, Transparency and Accountability* (Springer-Nature 2025); Belli, Nicolo Zingales, *Building sovereign and integrated data governance, from Latin America to the G20, International Data Privacy Law*, Volume 15, Issue 4, November 2025, Pages 319–322; Belli L. and others, *Soberania Digital e Inteligência Artificial no Brasil: Rumo à autonomia tecnológica* (Lumen-Juris 2026); Belli, L. *Data Sovereignty Doesn't Mean Data Isolationism*. Tech Policy press (15 July 2026).

² Belli, L. and Bhinder, A. *Cooperative Digital Sovereignty and Artificial Intelligence Promoting Resilience, Strategic Openness, and Self-Determination*. (Digital Cooperation Organization, 2026).

Yet despite its increasing use, data sovereignty remains an elusive and contested concept. Different actors employ the term to advance very different objectives. For some, it primarily concerns protecting individual privacy through robust data protection laws. Others understand it as ensuring state authority over data generated within national borders, often advocating localization requirements or restrictions on cross-border transfers.³ Still others frame data sovereignty as a matter of technological independence, emphasizing domestic cloud infrastructure, semiconductor production, artificial intelligence capabilities, or secure digital identities.

Increasingly, economists and international organizations recognize data as a strategic factor of production⁴ that underpins innovation, artificial intelligence and digital markets. This growing recognition has drawn attention to the concentration of data and digital infrastructures, raising concerns regarding competition, market power and innovation. At the same time, development scholars and international organizations such as UNCTAD have emphasized that the value generated by global data flows remains highly concentrated, with developing countries often contributing data while capturing only a limited share of the resulting economic benefits.⁵

These diverse understandings reveal that data sovereignty has become a multidimensional concept situated at the intersection of constitutional law, international law, cybersecurity, economics, technology policy and development studies. However, much of the existing literature – and the specialists that elaborate it – continues to analyse these dimensions separately, treating privacy, cybersecurity, industrial policy or digital infrastructure as distinct policy domains. This fragmentation obscures the broader transformation currently taking place in digital governance.

This paper argues that data sovereignty should instead be understood as an integrated governance framework. Building upon the definition proposed in previous research, we define data sovereignty as “the institutional capacity of individuals, societies and states to understand how data processing technologies work, develop alternatives and regulate them effectively, thus achieving

³ Brian Nougères, A. (2026). *International collection of personal data* (UN Doc. A/HRC/61/48). United Nations, Human Rights Council.

⁴ Mayer-Schönberger, V., & Cukier, K. (2013). *Big Data: A revolution that will transform how we live, work, and think*. Houghton Mifflin Harcourt.

⁵ UNCTAD. (2019) *Digital Economy Report 2019: Value Creation and Capture—Implications for Developing Countries*; UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development: For Whom the Data Flow*; World Bank. (2021). *World Development Report 2021: Data for Better Lives*. Washington DC: World Bank.

informational self-determination and fair redistribution of value, in accordance with democratically determined objectives.”⁶ Such objectives include the protection of fundamental rights, democratic accountability, economic development, technological innovation and healthy competition, cybersecurity and social justice.

This understanding deliberately departs from interpretations that reduce sovereignty to data localization.⁷ Localization may in certain circumstances contribute to sovereignty, particularly where national security or regulatory enforcement are concerned.⁸ However, localization alone cannot ensure meaningful control over data if the software, cloud infrastructure, hardware, standards and platforms through which data circulate remain externally controlled. A country may require that data remain physically within its territory while continuing to depend almost entirely upon foreign operating systems, cloud providers, payment infrastructures, artificial intelligence models and cybersecurity technologies. Conversely, a country may participate actively in cross-border data flows while maintaining substantial sovereign capacity through interoperable institutions, robust legal frameworks, domestic technological capabilities and diversified digital infrastructures.

Accordingly, this paper proposes a broader conception of sovereignty centred on governance capacity rather than territorial exclusivity. Namely, we contend that the concept of sovereignty, when applied to digital technologies, should be seen as the ability of individuals, societies and states to shape the rules governing data ecosystems and to exercise meaningful agency over digital transformation without becoming structurally dependent upon external technological, economic or political actors.⁹

⁶ Belli, L., Gaspar W.B. and Singh, S. (2024). Data sovereignty and data transfers as fundamental elements of digital transformation: Lessons from the BRICS countries. *Computer Law & Security Review*, vol. 54.

⁷ López González, J., Casalini, F., & Porras, J. (2022). *A Preliminary Mapping of Data Localisation Measures*. OECD Trade Policy Papers No. 262. OECD Publishing; Svantesson, D. (2020). *Data Localisation Trends and Challenges: Considerations for the Review of the Privacy Guidelines*. OECD Digital Economy Papers No. 301.

⁸ Yayboke, E., Ramos, C. G., & Sheppard, L. R. (2021). *The Real National Security Concerns over Data Localization*. Center for Strategic and International Studies (CSIS); López González, J., Casalini, F., & Porras, J. (2023). *The Nature, Evolution and Potential Implications of Data Localisation Measures*. OECD Trade Policy Papers No. 278. OECD Publishing; Greenleaf, G. (2023). *Personal Data Localisation and Sovereignty along Asia's New Silk Roads*. In A. Chander & H. Sun (Eds.), *Data Sovereignty: From the Digital Silk Road to the Return of the State*. Oxford University Press

⁹ In this perspective, see Luca Belli, 'To Get Its AI Foothold, Brazil Needs to Apply the Key AI Sovereignty Enablers (KASE)' in S Feldstein (ed), *New Digital Dilemmas: Resisting Autocrats, Navigating Geopolitics, Confronting Platforms* (Carnegie 2023); Belli, L. (2025). Exploring the Key AI Sovereignty Enablers (KASE) of Brazil, to Build an AI Sovereignty Stack. In: Luca Belli and Walter B Gaspar (eds), *The Quest for AI Sovereignty, Transparency and Accountability* (Springer-Nature

UPGRADING INFORMATIONAL SELF-DETERMINATION

The intellectual origins of this argument developed in this paper lie in the doctrine of informational self-determination. Developed by the German Federal Constitutional Court in its landmark 1983 Census Decision (*Volkszählungsurteil*), informational self-determination recognized that individuals must retain the ability to determine the disclosure and use of their personal information in order to preserve human dignity and democratic freedom.¹⁰ This essential principle¹¹ profoundly influenced European data protection law and later became embedded in the Charter of Fundamental Rights of the European Union and the General Data Protection Regulation (GDPR). Similar constitutional developments have subsequently emerged within the Inter-American human rights system.¹²

To date, informational self-determination remains an indispensable pillar of data protection. Privacy, dignity, autonomy and democratic participation continue to constitute the normative foundations of digital governance. Yet the digital economy, the geopolitical trends and the technological dependency dynamics of the twenty-first century differ fundamentally from the technological environment in which the doctrine was originally conceived.

The German Census Decision addressed the risks posed by centralized governmental databases during an era in which information processing remained relatively limited, largely national in scope, and information had not yet become a commodified asset.¹³ Contemporary digital ecosystems, by contrast, are

2025); Luca Belli, Nicolo Zingales, Building sovereign and integrated data governance, from Latin America to the G20, *International Data Privacy Law*, Volume 15, Issue 4, November 2025, Pages 319–322; Luca Belli and others, Soberania Digital e Inteligência Artificial no Brasil: Rumo à autonomia tecnológica (Lumen-Juris 2026).

¹⁰ Federal Constitutional Court of Germany (BVerfG), Judgment of 15 December 1983 (*Volkszählungsurteil* / Census Act Decision), Case Nos 1 BvR 209, 269, 362, 420, 440, 484/83, BVerfGE 65, 1.

¹¹ Brian Nogrères, A. (2022). Principles underpinning privacy and the protection of personal data (UN Doc. A/77/196). United Nations, General Assembly.

¹² Chiefly, the CAJAR case that will be debated in section 1.2. Inter-American Court of Human Rights, Case of the Members of the José Alvear Restrepo Lawyers' Collective (CAJAR) v Colombia (Preliminary Objections, Merits, Reparations, and Costs), Judgment of 18 March 2024, Series C No 522

¹³ In this latter perspective see Julie E Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford University Press 2019); Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Public Affairs 2019); Wayne Wei Wang, 'China's Digital Transformation: Data-Empowered State Capitalism and Social Governmentality' (2023) 31 *African Journal of Information and Communication* 1. In this latter perspective see Julie E Cohen, *Between Truth and Power: The Legal Constructions of Informational*

characterized by globally distributed and highly concentrated cloud computing, artificial intelligence (AI) ecosystems, ubiquitous sensors, algorithmic decision-making, platform economies, cross-border data flows and increasingly sophisticated cyber threats motivated by both financial and political purposes. Data have evolved from administrative records into one of the principal factors of production within the global economy. Their governance therefore raises questions extending far beyond individual privacy.

Today, the inability to secure digital infrastructures may compromise national sovereignty irrespective of the existence and strength of privacy legislation. Dependence upon foreign cloud providers may limit public sector autonomy even where personal data remain legally protected. Concentrated digital markets may reduce domestic innovation despite robust constitutional safeguards. Similarly, unequal taxation of highly digitalized business models may exacerbate wealth concentration while depriving governments of the fiscal resources needed to invest in secure and inclusive digital infrastructures.

These developments suggest that informational self-determination must be expanded rather than replaced. The core values underpinning the doctrine -human dignity, autonomy and democratic accountability- remain fully relevant. However, they must now be interpreted within a broader governance framework capable of addressing technological dependence, economic concentration, cybersecurity risks and developmental inequalities, without focusing exclusively on the protection of individual rights but also on collective interests, such as national security, economic development, healthy competition, innovation and scientific progress.¹⁴

Accordingly, this paper proposes a conception of data sovereignty that rests upon six mutually reinforcing dimensions:

- informational self-determination through robust data protection and fundamental rights;
- cybersecurity and digital resilience;
- technological sovereignty and Digital Public Infrastructure;
- industrial development and technological capabilities;

Capitalism (Oxford University Press 2019); Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Public Affairs 2019); Wang, W. W. 'China's Digital Transformation: Data-Empowered State Capitalism and Social Governmentality' (2023) 31 *African Journal of Information and Communication* 1.

¹⁴ In this perspective, see notably: Belli, L., Gaspar W.B. and Singh, S. (2024). Data sovereignty and data transfers as fundamental elements of digital transformation: Lessons from the BRICS countries. *Computer Law & Security Review*, vol. 54; Belli, Nicolo Zingales, Building sovereign and integrated data governance, from Latin America to the G20, *International Data Privacy Law*, Volume 15, Issue 4, November 2025, Pages 319–322; Belli L. and others, *Soberania Digital e Inteligência Artificial no Brasil: Rumo à autonomia tecnológica* (Lumen-Juris 2026).

- competition and innovation within digital markets;
- fiscal justice through taxation and mechanisms promoting equitable distribution of value generated by data.

These dimensions should not be understood as separate policy objectives. Rather, they constitute complementary components of a single governance architecture. Hence, exactly as strengthening one dimension may be well intentioned but not effective, weakness in any one dimension ultimately undermines sovereignty as a whole.

DATA SOVEREIGNTY AS GOVERNANCE CAPACITY

This multidimensional approach also challenges traditional understandings of sovereignty itself. Classical international law conceived sovereignty primarily in territorial terms.¹⁵ States exercised supreme authority within clearly defined geographic boundaries, while international law regulated relations between formally equal sovereign entities. Although territorial jurisdiction remains essential, digital technologies increasingly operate through transnational infrastructures that disregard conventional borders. Critical information infrastructure such as cloud computing, submarine cables, global platforms, AI models and international digital payment systems function across multiple jurisdictions simultaneously.

As a consequence, sovereignty can no longer be understood exclusively through territorial control. Effective governance increasingly depends upon industrial and institutional capacity, technological competence and choice, and international cooperation. States capable of maximising options of – including being able to develop – secure digital identities, interoperable payment systems, trusted data exchange platforms and resilient cybersecurity architectures may exercise considerably greater sovereignty than states relying entirely upon externally developed infrastructures, regardless of where data are physically stored.

This shift from territorial control to governance capacity has important normative implications. It suggests that sovereignty should not be measured by the volume of data retained within national borders, but by the ability to establish legitimate and effective frameworks governing their lifecycle. Such frameworks encompass legal protections, technological standards, institutional arrangements, market structures

¹⁵ Besson S. Sovereignty. in Peters A. & Wolfrum R. Max Planck Encyclopedias of International Law. Oxford University Press. (2021).

and fiscal policies. Data sovereignty therefore becomes a dynamic institutional and regulatory capability rather than a static territorial attribute.

Importantly, this conception avoids the false dichotomy between openness and sovereignty. Participation in global data flows need not diminish sovereignty provided that such participation occurs under conditions of meaningful choice, reciprocal cooperation and institutional resilience. Conversely, isolation from international digital ecosystems does not automatically enhance sovereignty if technological dependence merely shifts from one external actor to another.¹⁶

STRUCTURE OF THE PAPER

The remainder of this paper develops this argument in four sections. Section I examines the historical evolution of informational self-determination across different legal and political traditions. Beginning with the German Census Decision, it traces the subsequent incorporation of informational self-determination into European constitutional law, the Inter-American human rights system, Asian developmental approaches and African postcolonial critiques of digital dependency. The section demonstrates that while these traditions differ significantly, they share a common concern with preserving human and collective autonomy under conditions of expanding digital power.

Section II argues that contemporary digital transformation requires expanding informational self-determination into a broader conception of data sovereignty. It examines how cyber threats, AI evolutions, cloud computing dynamics, platform concentration and digital infrastructures fundamentally alter the conditions under which informational autonomy can be exercised.

Section III develops the paper's central analytical framework by examining the six interdependent dimensions of data sovereignty: data protection, cybersecurity, Digital Public Infrastructure, industrial policy, competition and innovation, and fiscal justice. Particular emphasis is placed on Digital Public Infrastructure as the technological architecture through which sovereign governance can be operationalized.

Finally, Section IV explores how sovereignty can be built through international cooperation rather than digital isolation. Drawing upon the principle of sovereign equality contained in Article 2 of the Charter of the United Nations, it argues that interoperable standards, shared governance frameworks and collaborative

¹⁶ Chander, A., & Lê, U. P. (2015). Data nationalism. *Emory Law Journal*, 64(3), 677-739.

institutional architectures provide the most promising pathway towards resilient and inclusive digital ecosystems.

The paper concludes by arguing that although contemporary digital infrastructures remain highly concentrated and geopolitical competition continues to intensify, data sovereignty should not be understood as an aspiration for technological autarky.¹⁷ Instead, it represents the collective capacity of states, societies and individuals to cooperate as equals in shaping the future of the global digital economy.

METHODOLOGY

This paper adopts an interdisciplinary legal and policy methodology combining doctrinal legal analysis with comparative institutional analysis and policy research. It draws upon primary legal sources, including constitutional provisions, legislation, judicial decisions, international instruments and policy documents, as well as academic literature from law, economics, political science, public administration, cybersecurity and digital governance. The objective is not to provide an exhaustive survey of each discipline, but to develop an integrated analytical framework capable of explaining data sovereignty as a multidimensional concept encompassing legal, technological, economic, developmental, cybersecurity and fiscal dimensions.

The paper also relies on comparative analysis to identify convergences and divergences across different regulatory traditions, with particular attention to European, American, Asian and African approaches to informational self-determination and data governance. In addition, it examines contemporary international initiatives relating to Digital Public Infrastructure (DPI), data governance and digital cooperation in order to identify emerging principles of interoperability and cooperative sovereignty.

Generative Artificial Intelligence was employed as a research support tool during the preparation of this manuscript. Specifically, it was used to assist in synthesising the authors' previous research, improving the structure and coherence of the manuscript, identifying potentially relevant literature for subsequent verification, refining language and style, and facilitating the organisation of references

¹⁷ Belli, L. Data Sovereignty Doesn't Mean Data Isolationism. Tech Policy press (15 July 2026).

1. FROM INFORMATIONAL SELF-DETERMINATION TO DATA SOVEREIGNTY

The contemporary debate on data sovereignty finds its normative roots in one of the most influential constitutional decisions of the twentieth century: the judgment of the German Federal Constitutional Court of 15 December 1983 concerning the Federal Census Act (*Volkszählungsurteil*).¹⁸ Although decided in response to a seemingly ordinary administrative census, the case fundamentally transformed constitutional understandings of privacy, personal autonomy and state power in what was already starting to be defined as “information society”¹⁹.

The controversy arose after the Federal Republic of Germany enacted legislation authorizing the collection of extensive personal information through the national census. Several citizens challenged the legislation, arguing that the accumulation and potential combination of personal information by public authorities created risks that extended well beyond the immediate purposes of statistical administration. The Court's reasoning reflected not only concerns about technological change but also the constitutional lessons derived from Germany's historical experience with authoritarian surveillance during both the National Socialist regime and the German Democratic Republic. The judgment therefore recognized that democratic freedom depends upon limiting informational asymmetries between individuals and the state.

The Court articulated a constitutional principle that would become known as the right to informational self-determination (*informationelle Selbstbestimmung*). Deriving this right from the guarantees of human dignity and the free development of personality contained in Articles 1 and 2 of the Basic Law, the Court held that individuals must retain the authority to determine, in principle, the disclosure and use of their personal information. Deriving this right from the guarantees of human dignity and the free development of personality contained in Articles 1 and 2 of the German Basic Law, the Court held that individuals must retain the authority to determine, in principle, the disclosure and use of their personal information. Without such authority, citizens would be unable to anticipate how information about them might be combined, interpreted or used in the future. This uncertainty, the Court reasoned, would inevitably discourage individuals from exercising an

¹⁸ Federal Constitutional Court of Germany (BVerfG), Judgment of 15 December 1983 (*Volkszählungsurteil* / *Census Act Decision*), Case Nos 1 BvR 209, 269, 362, 420, 440, 484/83, BVerfGE 65, 1.

¹⁹ See, as an instance, the seminal report Nora D. & Minc A. *L'informatisation de la société. Rapport à M. le Président de la République*. La Documentation française. 1978

ample range of fundamental freedoms, participating in democratic life or expressing dissenting opinions.

Importantly, the significance of the Census Decision extended far beyond the recognition of a new privacy right. It represented a profound reconceptualization of constitutional liberty under conditions of information processing. Rather than viewing privacy merely as “the right to be let alone”²⁰ underpinning a legitimate claim of private life protection and confidentiality, the Court understood the informational dimension of autonomy as requiring meaningful control over the circulation and use of personal information. In this perspective, freedom in the information society depended not simply upon preventing disclosure but upon preserving the individual's capacity to make informed choices regarding the governance of personal data.

This insight proved remarkably prescient. Long before the emergence of the internet, cloud computing, Big Data analytics or AI, the Court anticipated that the aggregation of apparently innocuous pieces of information could fundamentally alter the relationship between citizens and public authority.²¹ Informational power, rather than physical coercion alone, became recognized as a central dimension of constitutional governance.

The doctrine of informational self-determination subsequently exerted profound influence on European data protection law, shaping legislative developments across the continent and providing the philosophical foundation upon which contemporary digital rights would later be constructed.²² At the same time, its emphasis on individual autonomy reflected the technological and political realities of the early 1980s. The principal concern was the relationship between the citizen and the state. Markets for personal data were still in their infancy, global digital platforms did not yet exist, and cybersecurity had not emerged as a central policy concern.

As later sections of this study will argue, these transformations require neither abandoning nor replacing informational self-determination, which acquires an even more relevant role. However, the recent technological challenges as well as the geopolitical dimension that technological dependencies have acquired, demand the

²⁰ Warren S. & Brandeis L. The Right to Privacy. Harvard Law Review, Vol. 4, No. 5 (Dec. 15, 1890), pp. 193-220

²¹ Benkler, Y. (2006). *The wealth of networks: How social production transforms markets and freedom*. Yale University Press.

²² Streinz T. The Evolution of European Data Law" in Craig P. and de Búrca G. (eds), *The Evolution of EU Law* (Oxford University Press, 3rd edn 2021) chapter 29.

expansion of this initial conception of informational self-determination into a richer and more comprehensive conception of data sovereignty.

1.1. INFORMATIONAL SELF-DETERMINATION FROM CONSTITUTIONAL PRINCIPLE TO REGULATORY MODEL

The doctrine of informational self-determination articulated by the German Federal Constitutional Court rapidly transcended its national origins to become one of the defining principles of European digital governance.²³ Although the concept itself remained rooted in German constitutional jurisprudence, its underlying values of human dignity, autonomy and democratic participation progressively informed the development of European Union law, transforming data protection from an administrative concern into a constitutional commitment.

This evolution reflected the broader European constitutional project. Following the Second World War, European integration was built upon the conviction that economic cooperation should be accompanied by the protection of fundamental rights and the rule of law. As digital technologies expanded during the final decades of the twentieth century, the European institutions increasingly recognised that the protection of personal information constituted an essential precondition for the effective enjoyment of individual liberty within an integrated internal market.²⁴

The adoption of Directive 95/46/EC represented a decisive step in this direction. While primarily intended to harmonise national legislation to facilitate the free movement of personal data within the European Union, the Directive also reflected a deeper constitutional ambition. Personal data were no longer treated simply as commercial information but as an extension of individual personality deserving legal protection irrespective of economic considerations. The Directive therefore established common principles governing the collection, processing and transfer of personal data while simultaneously facilitating the functioning of the internal market.

The constitutionalisation of data protection reached a new stage with the Charter of Fundamental Rights of the European Union.²⁵ Significantly, the Charter distinguished between respect for private life, protected under Article 7, and the protection of personal data under Article 8. This distinction was unprecedented in

²³ Brian Nogrères, A. (2022). Principles underpinning privacy and the protection of personal data (UN Doc. A/77/196). United Nations, General Assembly.

²⁴ Erdos D. "The Development of European Data Protection Law and Regulation" in Erdos D. European Data Protection Regulation, Journalism, and Traditional Publishers. (Oxford University Press, 2019).

²⁵ Ibid and supra n (17).

comparative constitutional law. Rather than considering data protection merely as one aspect of privacy, the European Union recognised it as an autonomous fundamental right with its own normative content. Article 8 further established that personal data must be processed fairly, for specified purposes and on the basis of consent or another legitimate legal ground, while guaranteeing access and rectification rights under the supervision of independent authorities.

This constitutional architecture subsequently found its most comprehensive expression in the General Data Protection Regulation (GDPR). Entering into force in 2018, the GDPR sought not only to harmonise European data protection law but also to respond to the emergence of global digital platforms, large-scale algorithmic processing and increasingly complex cross-border data flows. The Regulation significantly expanded the range of individual rights through mechanisms such as data portability, the right “to be forgotten” or right to erasure, increased accountability obligations, privacy by design and by default, and restrictions on automated decision-making. At the same time, strengthened supervisory authorities and introduced substantial administrative sanctions.

The global significance of the GDPR extends well beyond Europe. Through its extraterritorial application, adequacy mechanisms and influence on national legislation across multiple jurisdictions, the Regulation has contributed to what scholars frequently describe as the “Brussels Effect”²⁶: the capacity of European regulation to shape global data governance through market power and regulatory lobbying rather than territorial coercion.²⁷ Countries across Latin America, Africa and Asia have increasingly aligned domestic legislation with GDPR principles to facilitate international trade and data transfers, making European data protection standards an important reference point in global regulatory convergence.²⁸

Nevertheless, despite its remarkable achievements, the European model remains fundamentally centred upon the relationship between individuals and those processing their personal data. Its principal objective is to protect individual autonomy against unlawful or disproportionate data processing. The degree to which current data protection framework are able to achieve such goal effectively rather than providing a mere facade of compliance is the object of intense debates²⁹

²⁶ Bradford, A. ‘The Brussels Effect’ (2012) 107 Nw U L Rev 1, 3, 6.

²⁷ Bradford, A. *The Brussels Effect: How the European Union Rules the World* (2020).

²⁸ Brian Nougères, A. (2022). *Privacy and personal data protection in Ibero-America: A step towards globalization?* (UN Doc. A/HRC/49/55). United Nations, Human Rights Council; Carrillo A.J. and Jackson, M. Follow the Leader? A Comparative Law Study of the EU’s General Data Protection Regulation’s Impact in Latin America. *ICL Journal* 2022; 16(2): 177–262.

²⁹ Li W. and others. Mapping the empirical literature of the GDPR’s (In-)effectiveness: A systematic review. *Computer Law & Security Review*. 57 (2025) 106129

and may lead to question data protection law capacity to concretely guarantee individual rights.

Furthermore, although the GDPR contains important provisions relating to security, accountability and international transfers, it does not directly address broader questions concerning technological dependence, industrial capability, market concentration or geopolitical asymmetries within the digital economy. These issues increasingly fall outside the conceptual boundaries of informational self-determination as traditionally understood.

Recent European initiatives – including the Data Governance Act, the Data Act, the Digital Markets Act, the Digital Services Act, the Artificial Intelligence Act, the Cloud Sovereignty framework and the European strategy for Digital Public Infrastructure – suggest that the European Union itself has begun moving beyond a purely privacy-centred approach. Collectively, these instruments seek to regulate data not merely as an object of individual rights but as an economic resource, a strategic asset and a component of critical infrastructure³⁰. In doing so, European digital governance increasingly reflects a broader conception of sovereignty, even if this evolution has not yet been fully articulated in conceptual terms.

1.1.1. INFORMATIONAL SELF-DETERMINATION IN THE INTER-AMERICAN HUMAN RIGHTS SYSTEM

Developments within the Inter-American human rights system reveal a parallel yet distinct evolution of informational self-determination. Although Latin American constitutional traditions have historically placed strong emphasis on privacy and “habeas data”³¹, the emergence of digital technologies has progressively expanded the understanding of personal data protection within the framework of human rights.

A particularly significant milestone is the jurisprudence of the Inter-American Court of Human Rights, which has increasingly recognised that the collection, processing and dissemination of personal information directly affect the exercise of fundamental freedoms guaranteed by the American Convention on Human Rights. Rather than viewing personal data merely as objects of administrative regulation,

³⁰ Plantin, J. C., Lagoze, C., Edwards, P. N., & Sandvig, C. (2018). Infrastructure studies meet platform studies in the age of Google and Facebook. *New Media & Society*, 20(1), 293-310

³¹ Alvim Wambier T.A. (Ed.), *Habeas Data*. São Paulo: RT, 1998; Guadamuz, A. *Habeas Data: The Latin-American Response to Data Protection*. *The Journal of Information Law and Technology*. v. 2, 2000.

the Court has linked informational autonomy to the effective enjoyment of dignity, freedom of expression, freedom of association and democratic participation.

This evolution finds important expression in the *CAJAR* judgment, in which the Court recognised that the protection of personal information forms part of the broader guarantee of private life under Article 11 of the American Convention. This evolution finds important expression in the *CAJAR* judgment³², in which the Court recognised that the protection of personal information forms part of the broader guarantee of private life under Article 11 of the American Convention. The decision is particularly noteworthy because it situates informational self-determination within the broader constitutional framework of democratic society. Surveillance, unlawful collection of personal information and arbitrary processing practices do not simply interfere with privacy; they may also undermine civic participation, discourage political engagement and weaken democratic institutions.

The Inter-American approach therefore complements the European model while introducing a particular emphasis upon democratic accountability and the protection of human rights defenders, journalists and civil society actors. In societies marked by recent history of authoritarianism, political violence and structural inequality, informational self-determination assumes a particularly important role in safeguarding democratic participation against both public and private abuses of power.

Latin American constitutional practice also demonstrates an important openness towards recognising digital rights as extensions of broader constitutional guarantees. Several constitutions explicitly protect habeas data, providing individuals with rights to access, correct and update information concerning themselves held in public or private databases.³³ Although these mechanisms differ institutionally from European data protection authorities, they pursue similar objectives by reinforcing individual agency over personal information.

At the same time, however, many Latin American countries confront challenges that extend beyond the traditional boundaries of privacy law. Together with low institutional maturity and literacy (especially about data protection and the functioning of technologies), limited domestic technological capacity, dependence upon foreign cloud providers, concentration of digital markets and unequal participation in the global data economy raise questions that informational self-

³² Chiefly, the *CAJAR* case that will be debated in section 1.2. Inter-American Court of Human Rights, *Case of the Members of the José Alvear Restrepo Lawyers' Collective (CAJAR) v Colombia* (Preliminary Objections, Merits, Reparations, and Costs), Judgment of 18 March 2024, Series C No 522

³³ Carrillo A.J. and Jackson, M. Follow the Leader? A Comparative Law Study of the EU's General Data Protection Regulation's Impact in Latin America. *ICL Journal* 2022; 16(2): 177–262.

determination is far from being properly addressed. Consequently, digital policy debates have increasingly connected personal data protection with digital industrial policy, cybersecurity, digital inclusion and technological cooperation.³⁴

In this respect, the Inter-American experience illustrates a broader global trend. Protection of personal information has been elevated to the rank of essential constitutional objective, but it has become evident that a sustainable governance of digital transformation increasingly requires integrating human rights with questions of economic development, cybersecurity, technological capability and institutional resilience.

1.2. CONSIDERING THE ASIAN PERSPECTIVES: A COLLECTIVE APPROACH TO INFORMATIONAL SELF-DETERMINATION FOR SECURITY AND DEVELOPMENT

Unlike the European and Inter-American conceptions, where informational self-determination developed primarily as an individual constitutional right limiting the exercise of state power, many Asian approaches to data governance have evolved within a broader conception of the relationship between the individual, society and the state, with a much more pronounced focus on collective interests. Indeed, although considerable diversity exists across the region, digital governance has frequently been framed not only in terms of protecting individual rights but also of promoting social stability, national security, economic modernization and technological development.³⁵

This divergence reflects distinct constitutional traditions and developmental trajectories. Many Asian economies experienced rapid industrialization under developmental states that actively coordinated technological upgrading, industrial policy and infrastructure investment. Consequently, digital technologies have often

³⁴ Belli, L. & Bhinder. Cooperative Digital Sovereignty and Artificial Intelligence Promoting Resilience, Strategic Openness, and Self-Determination. Digital Cooperation Organization (2026); Belli L. Soberania Digital no Brasil Diagnóstico, Desafios e Caminhos sob a perspectiva da Ciência, Tecnologia e Inovação. Centro de Gestão e Estudos Estratégicos (CGEE). MCTI (Ministério da Ciência, Tecnologia e Inovação Brasília. (2026).

³⁵ Greenleaf, G. (2014). Asian data privacy laws: Trade and human rights perspectives. Oxford University Press; Bo Zhao a , Yang Feng Mapping the development of China's data protection law: Major actors, core values, and shifting power relations. Computer Law & Security Review 40 (2021) 105498; Wang, W. 'China's Digital Transformation: Data-Empowered State Capitalism and Social Governmentality' (2023) 31 African Journal of Information and Communication 1; Belli L. & Chang S. Governança de dados na China: soberania, cibersegurança e proteção de dados rumo ao "Efeito Pequim". Revista Brasileira de Direitos Fundamentais & Justiça. v. 23 n. 52 (2025).

been viewed as strategic assets contributing to national development rather than solely as domains requiring legal protection against governmental interference.

Countries such as Singapore, the Republic of Korea, Japan, China and, more recently, India illustrate different manifestations of this approach. Singapore's digital governance strategy, for example, combines personal data protection with strong emphasis on trusted digital infrastructure, cybersecurity and innovation ecosystems.³⁶ The Personal Data Protection Act coexists with comprehensive national initiatives promoting digital identity, interoperable public services and secure digital transactions, reflecting an integrated understanding of digital governance.

Similarly, the Republic of Korea has historically linked digital transformation to industrial competitiveness.³⁷ Government investment in broadband infrastructure, semiconductor manufacturing, artificial intelligence and cybersecurity has been accompanied by regulatory frameworks seeking to balance privacy protection with innovation. Here, informational self-determination operates alongside an explicit commitment to technological capability and economic resilience.

Japan has adopted a comparable approach through its vision of "Data Free Flow with Trust" (DFFT), promoted during its G20 Presidency in 2019, and subsequently endorsed and fostered by the OECD³⁸. Rather than advocating unrestricted data flows or strict localization requirements, DFFT seeks to reconcile openness with trust by combining international interoperability, privacy protection, cybersecurity and common governance standards. This initiative illustrates an important

³⁶ Arif Perdana and Intan Azura Mokhtar, 'Digital Transformation in Government: Lessons from GovTech Singapore' (2025) *Journal of Information Technology Teaching Cases* 1 ; Wanning Sun, 'Artificial Intelligence: Governing Singapore's Smart Digital Journey' (2024) 10(3) *Communication Research and Practice*

³⁷ Keun Lee, *The Art of Economic Catch-up: Barriers, Detours and Leapfrogging in Innovation Systems* (Cambridge University Press 2019); Keun Lee, 'How Can Korea Be a Role Model for Catch-up Development? A "Capability-based" View' (2019) 47(2) *Oxford Development Studies* 164–17.

³⁸ The DFFT concept prescribes that ensuring trust in terms of privacy, security, and intellectual property rights is a prerequisite for the free flow of data across borders. See G20. "G20 Leaders' Declaration in Osaka". (June 29, 2019). Under the 2023 Japanese presidency, also the G7 Summit in Hiroshima endorsed the "Vision of the G7 Ministers of Technology and Digital to operationalize the free flow of data with confidence and its priorities," including the establishment of an "Institutional Partnership Agreement." See G7. Ministerial Declaration - The Meeting of the G7 Digital and Technology Ministers. (04/30/2023). In this context, the G7 Declaration of Ministers of Technology and Digital further stated that "the attributes of the OECD and its current work in the areas of data governance, privacy, free flow of data with trust, and the digital economy make it suitable to advance this international effort" See G7. Annex 1 of the digital and technology track – G7 vision to operationalize the DFFT and its priorities. (04/30/2023).

conceptual shift: sovereignty is not achieved through isolation but through participation in trusted digital ecosystems governed by shared rules.³⁹

In China, digital governance has developed within a constitutional framework placing greater emphasis on collective interests, national security and state-led development.⁴⁰ Legislation such as the Cybersecurity Law, the Data Security Law and the Personal Information Protection Law demonstrates that China recognizes privacy and personal information protection as important legal values. However, these objectives are explicitly integrated with broader goals concerning national security, industrial competitiveness and technological sovereignty.

While the institutional arrangements differ substantially from liberal constitutional traditions, the Chinese experience nevertheless underscores an important point for the present analysis: data governance increasingly extends beyond individual privacy to encompass technological capability, cybersecurity and economic development.⁴¹ Whether pursued through liberal democratic institutions or more centralized governance models, contemporary states increasingly recognise that data constitute strategic infrastructure requiring coordinated public governance.

Perhaps the most significant recent development has emerged in India through the construction of what has become known as the India Stack.⁴² Combining digital identity (Aadhaar), digital payments (UPI), document authentication, consent-based data sharing and other interoperable digital public infrastructures, India has demonstrated that governments can create foundational digital architectures that simultaneously promote inclusion, innovation and public service delivery..Although debates surrounding privacy, surveillance and exclusion remain important, the Indian experience has fundamentally altered international discussions concerning the relationship between technological infrastructure, data governance and sovereignty.⁴³

The concept of Digital Public Infrastructure (DPI), now increasingly promoted by the G20, the United Nations Development Programme and numerous development institutions, owes much to this experience. Rather than relying exclusively upon regulation to shape digital markets, DPI seeks to embed normative values directly within technological architecture. Digital identity systems, payment infrastructures

³⁹ Chander, A., & Lê, U. P. (2015). Data nationalism. *Emory Law Journal*, 64(3), 677-739.

⁴⁰ Wang. W.W. Chang S. Chen S. Assessing the Chinese Personal Information Protection Law (PIPL) and Beyond: The Stakeholder Architecture of Data Protection in China. in Belli L. & Gaspar W. Personal Data Architectures in the BRICS countries. (Oxford University Press 2025)

⁴¹ Idem.

⁴² Parsheera S. Stack is the New Black?: Evolution and Outcomes of the 'India-Stackification' Process. *Computer Law & Security Review*, 52 (2024) 105947

⁴³ Parsheera S. "Awaiting the Dawn of Data Protection Regulation in India" in Belli L. & Gaspar W. Personal Data Architectures in the BRICS countries. (Oxford University Press 2025)

and trusted data exchange mechanisms become institutional infrastructures supporting both individual rights and economic development.

Taken together, these diverse Asian experiences reveal that informational self-determination alone provides only a partial account of digital governance. Protection of individual rights remains important, but effective governance increasingly requires integrating privacy with cybersecurity, technological infrastructure, industrial policy and both technical and legal interoperability. In this respect, Asian experiences contribute significantly to the broader evolution from an individual-centered conception of informational self-determination toward a more complex notion of data sovereignty.

1.3. AN AFRICAN PERSPECTIVE: DATA SOVEREIGNTY AS RESISTANCE TO DIGITAL COLONIALISM

If European constitutionalism emphasises individual autonomy and many Asian approaches integrate development with technological capability, African scholarship contributes a different but equally important perspective by locating data governance within the historical experience of colonialism, dependency and unequal participation in the global political economy.⁴⁴

The emergence of the digital economy has generated growing concern that historical patterns of extraction characterizing colonial rule may be reproduced through contemporary digital technologies.⁴⁵ Instead of extracting natural resources, colonial powers and multinational corporations increasingly derive value from data generated by populations whose countries possess limited capacity to govern, process or economically benefit from those resources. This phenomenon has been described by numerous scholars as data colonialism⁴⁶, emphasising the continuity between historical systems of economic extraction and contemporary digital capitalism.

Among the most influential contributions to this debate is the work of Everisto Benyera, who argues that the Fourth Industrial Revolution risks reproducing

⁴⁴ See notably Benyera, E. *The Fourth Industrial Revolution and the Recolonisation of Africa: The Coloniality of Data*. (Routledge, 2021).

⁴⁵ Avila Pinto, R. (2018). Digital sovereignty or digital colonialism? New tensions of privacy, security and national policies. *SUR: International Journal on Human Rights*, 15(27), 15–27; Ricaurte, P. (2019). Data epistemologies, the coloniality of power, and resistance. *Television & New Media*, 20(4), 350–365; Nothias T, “An Intellectual History of Digital Colonialism” [2025] *The Journal of Communication*.

⁴⁶ Couldry, N., & Mejias, U. A. (2019). *The costs of connection: How data is colonizing human life and appropriating it for capitalism*. Stanford University Press.

colonial relationships through the concentration of technological infrastructure, intellectual property, cloud computing, AI and data processing capacities outside the African continent.⁴⁷ In this perspective, data become not merely an object of regulation but a strategic resource whose external appropriation reinforces structural dependency.

The African critique therefore broadens the concept of informational self-determination in two important respects. First, it shifts attention from the rights of individuals to the agency of entire societies and states. While personal privacy remains important, the principal concern is whether African countries possess meaningful capacity to determine how data generated within their economies contribute to domestic development rather than external accumulation of power and wealth. Questions concerning data localization, domestic cloud infrastructure, regional digital markets and local technological capability thus acquire developmental significance extending beyond conventional privacy law.

Second, African scholarship has the relevant merit of explicitly connecting digital governance with economic justice.⁴⁸ The value generated through data-intensive business models is overwhelmingly concentrated within a relatively small number of multinational technology firms headquartered outside the continent. Consequently, African societies contribute raw data while capturing only a small fraction of the resulting economic value. This asymmetry mirrors historical patterns whereby colonies exported raw materials while industrial value creation occurred elsewhere.⁴⁹

These concerns have increasingly informed regional initiatives such as the African Union's Data Policy Framework and broader efforts to support digital transformation under the African Continental Free Trade Area (AfCFTA).⁵⁰ Rather than advocating digital autarky, these initiatives seek to strengthen regional capacity through common regulatory frameworks, interoperable digital markets and investment in digital infrastructure. Sovereignty is therefore understood as the capacity to participate more equitably in the global digital economy rather than withdrawing from it.

⁴⁷ Benyera, E. *The Fourth Industrial Revolution and the Recolonisation of Africa: The Coloniality of Data*. (Routledge, 2021).

⁴⁸ Folashadé Soulé, *Digital Sovereignty in Africa: Moving beyond Local Data Ownership* (CIGI Policy Brief No 185, Centre for International Governance Innovation, 25 June 2024)

⁴⁹ Idem.

⁵⁰ Kweku Adams, Rexford Attah-Boakye, Honglan Yu, Irene Chu and Dafydd Mali, 'African Continental Free Trade Area and Regional Trade in ICT and Digital Technologies' (2024) 30(4) *Journal of International Management*

Importantly, the African perspective introduces an explicit developmental dimension that has often remained implicit within European privacy debates. Protecting personal information, although essential, does not by itself guarantee technological capability, domestic innovation or economic transformation. A country may adopt sophisticated data protection legislation while remaining almost entirely dependent upon foreign cloud providers, software ecosystems, payment infrastructures and Ai models. In such circumstances, data protection law only provides a formal appearance of sovereignty, coexisting with highly effective private ordering defined by private tech companies, which becomes the most effective form of regulation thus consecrating a form of private sovereignty⁵¹

The African contribution therefore reinforces one of the central arguments advanced in this paper: data sovereignty cannot be reduced to legal rights alone. It also requires institutional capacity, technological capability and economic structures capable of generating public value from data. Without these complementary elements, informational self-determination risks becoming a formally recognised right whose practical exercise remains constrained by structural dependency.

1.4. CONVERGING TRADITIONS, DIVERGING EMPHASES

The comparative analysis developed above demonstrates that informational self-determination has followed distinct historical trajectories across different legal and political traditions. In Europe, the concept emerged primarily as a constitutional safeguard protecting individual autonomy against excessive data processing. The Inter-American system similarly grounds informational self-determination in human dignity but places greater emphasis upon democratic participation and the protection of civil society within contexts shaped by authoritarian experiences.

Many Asian approaches, while increasingly recognising personal data protection, integrate privacy with broader objectives concerning national security, technological modernization and economic development. African scholarship, in turn, introduces a postcolonial critique that links data governance with dependency, unequal value extraction and developmental justice. These traditions differ considerably in their normative priorities, institutional arrangements and political contexts. Nevertheless, they share a common underlying concern: preserving meaningful human and collective agency within increasingly data-driven societies.

This convergence is significant because it suggests that the debate has gradually shifted from whether data require governance to how governance should be organised. In each region, the core elements of informational self-determination

⁵¹ Belli, L. Structural power as a critical element of digital platforms' private sovereignty. In E. Celeste, A. Heldt & C. Iglesias Keller (Eds.), *Constitutionalising social media* [pages]. (Hart, 2022).

have progressively expanded beyond an original focus on data privacy. The questions confronting policymakers today are no longer limited to whether individuals should control their personal information. Increasingly, they concern whether societies possess the institutional, technological and economic capacity to govern digital transformation itself.

It is precisely at this point that the concept of data sovereignty becomes necessary. Informational self-determination remains its normative foundation, but leveraging only its individual-centered dimension is no longer sufficient to frame the complex governance challenges generated by AI, cloud computing, platform economies, cyber conflict and global digital infrastructures. Hence, data sovereignty should not be understood as replacing informational self-determination. Rather, it represents its logical evolution under the conditions of the contemporary digital economy and geopolitics.

2. WHY AN EXCLUSIVELY INDIVIDUALISTIC CONCEPTION OF INFORMATIONAL SELF-DETERMINATION IS NO LONGER SUFFICIENT

The comparative analysis developed in the previous section demonstrates that informational self-determination has become a cornerstone of contemporary digital governance, reflecting a shared commitment to preserving human autonomy in increasingly data-driven societies. Yet the same comparative analysis also reveals a more subtle transformation. Although the macrothese legal traditions briefly presented above begin from the protection of the individual, none remains confined to an exclusively individualistic understanding of digital governance.

Across different jurisdictions, concerns relating to national security, cybersecurity, technological dependencies and capabilities, economic development, industrial policy and international cooperation have progressively expanded the scope of digital regulation. Hence, informational self-determination continues to provide the normative foundation, but it no longer exhausts the range of interests implicated by the contemporary data economy.

This evolution is hardly surprising. The doctrine of informational self-determination emerged during the early stages of computerisation, when constitutional concerns centred primarily upon the collection and processing of personal information by public authorities. The German Census Decision was decided in an era characterised by technologic, economic and geopolitical dynamics radically different from the current ones. At that time, personal data constituted the principal object of regulation, and the principal constitutional question concerned the relationship between the individual and the State.

The technological environment has since undergone a profound transformation. Data have become not only objects of legal protection but also strategic economic assets, essential inputs into AI systems, foundations of digital public services, drivers of industrial innovation and, increasingly, instruments of geopolitical influence. Equally important, digital infrastructures themselves have acquired strategic significance, whose governance directly affects national resilience and economic competitiveness. Under these conditions, an exclusively individualistic conception of informational self-determination becomes insufficient for at least three reasons.

First, it aims at regulating only one dimension of increasingly complex digital ecosystems. Data protection law primarily targets – not necessarily effectively⁵² – the relationship between data subjects and those processing their personal information. The guarantees it establishes remain indispensable for protecting individual autonomy. However, they do not determine who owns, operates and can extract value from cloud infrastructures and under which conditions, who develops and has access to foundational AI models, who controls digital payment systems or how value generated through data-intensive activities is redistributed. Questions concerning technological capability, market structure, industrial development and data taxation remain largely outside the scope of classical privacy law.⁵³

Second, an individualistic conception inadequately addresses the collective nature of many contemporary digital risks.⁵⁴ Cybersecurity provides perhaps the clearest illustration. A successful cyberattack compromising the information confidentiality, integrity and availability of a national payment system, an electricity grid or a government digital public service may compromise the security and autonomy of millions of individuals simultaneously, regardless of whether their personal data were processed lawfully under applicable privacy legislation. Similarly, dependence upon foreign cloud providers subject to foreign jurisdiction create systemic risks of service continuity that cannot be resolved through individual consent or data

⁵² David Erdos, 'Acontextual and Ineffective? Reviewing the GDPR Two Years On' (International Forum for Responsible Media, 2020); Ryan, J. 'Europe's Governments Are Failing the GDPR: Brave's 2020 Report on the Enforcement Capacity of Data Protection Authorities' (2020); Karjalainen, T. 'The Battle of Power: Enforcing Data Protection Law against Companies Holding Data Power' (2022) 47 Computer Law & Security Review 105742.

⁵³ Belli L., Fossati G. McClaskey L. and Zingales, N. Proteção, Tributação e Equidade de Dados: Equilibrando Valores, Riscos e Obrigações na Economia Digital. (Lumen Juris 2026)

⁵⁴ Belli L. and others, Soberania Digital e Inteligência Artificial no Brasil: Rumo à autonomia tecnológica (Lumen-Juris 2026); Belli, L. and Bhinder, A. Cooperative Digital Sovereignty and Artificial Intelligence Promoting Resilience, Strategic Openness, and Self-Determination. (Digital Cooperation Organization, 2026).

protection rights alone. Indeed, the resilience and security of digital ecosystems has become a public good requiring collective governance.⁵⁵

Third, an individual perspective to informational self-determination says relatively little about the political economy of data. The extraordinary concentration of digital markets among a limited number of global technology firms has generated unprecedented asymmetries in economic power, technological capability and control over digital infrastructures. These asymmetries affect not only competition but also the capacity of states to pursue independent digital policies, foster domestic innovation and ensure that the value generated through data contributes to sustainable and inclusive development. From this perspective, sovereignty concerns not merely the protection of individuals but also the sustainability of markets, national infrastructures and innovation systems.

Taken together, these developments suggest that the contemporary challenge is no longer simply protecting individuals from excessive data processing. It is ensuring that societies possess the institutional capacity to govern digital transformation itself. Hence, while providing the conceptual and constitutional foundation upon which a broader conception of data sovereignty must be constructed, a mere individualistic conception of informational self-determination remains is not sufficient to ensure what we define as data sovereignty, i.e. the capacity to understand how data processing technologies work, develop alternatives and regulate them effectively..

This broader conception does not abandon the individual. On the contrary, it seeks to preserve individual autonomy by recognising that such autonomy increasingly depends upon conditions extending well beyond data privacy law. Meaningful informational self-determination today presupposes secure digital infrastructures, competitive markets, trusted technological architectures, cybersecure infrastructures and resilient public institutions and equitable participation in the economic value generated by data. Individual rights and collective governance therefore must not be seen as competing objectives but mutually reinforcing components of the same constitutional project.

The transition from informational self-determination to data sovereignty should thus be understood as analogous to earlier developments in constitutional theory. Liberal constitutions initially emerged to protect individuals against arbitrary governmental power. Over time, however, constitutional governance expanded to include social rights, economic regulation, public administration and institutional accountability, reflecting the growing complexity of modern societies.⁵⁶

⁵⁵ DeNardis, L. (2020). *The internet in everything: Freedom and security in a world with no off switch*. Yale University Press

⁵⁶ Katharine G. Young, *Constituting Economic and Social Rights* (Oxford: Oxford University Press, 2012).

The evolution of digital governance follows a similar trajectory. Informational self-determination remains its constitutional nucleus, but contemporary digital societies require a broader governance framework capable of integrating rights, technological innovation, (cyber)technology, security, economic development and democratic accountability. It is this multidimensional governance framework that this paper describes as data sovereignty.

3. THE CONSTITUTIVE DIMENSIONS OF DATA SOVEREIGNTY

The previous section argued that informational self-determination remains the indispensable normative foundation of digital governance, but that it is no longer sufficient to address the structural transformations produced by the contemporary data economy, digital dependencies and geopolitical tensions. While individual rights remain essential, it is either overconfident or naïve to assume that, by themselves, they can effectively determine how public authority, technological infrastructures, markets and institutions should be organised. The central question is therefore no longer simply how individuals may exercise control over personal information, but how democratic societies can develop the institutional capacities required to govern digital transformation in the public interest.

This section advances the central theoretical proposition of the paper: data sovereignty should not be understood as a single legal principle, a technological objective or a policy instrument achievable through data localisation, domestic infrastructure or stronger privacy legislation alone. It is better understood as an integrated institutional capacity generated by the interaction of multiple governance dimensions. Each dimension addresses a distinct source of vulnerability within digital ecosystems, yet none is sufficient in isolation. Sovereignty arises only when these capacities reinforce one another and enable states and societies to exercise meaningful agency over the legal, technological, economic and organisational conditions through which data are generated, extracted, exchanged and transformed into value.⁵⁷

Building upon this understanding, the section identifies six constitutive dimensions of data sovereignty: (i) data protection; (ii) cybersecurity and digital resilience; (iii) Digital Public Infrastructure; (iv) industrial development and technological capability; (v) competition and innovation; and (vi) fiscal justice. Conspicuously,

⁵⁷ Cohen, J.E. *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford University Press 2019); Zuboff, S. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Public Affairs 2019).

these dimensions should not be interpreted as isolated policy sectors, but as complementary institutional capacities through which sovereign agency is progressively constructed and sustained.

This multidimensional perspective also reflects the growing complexity of information governance itself. Data protection without resilient infrastructures cannot preserve trust. Cybersecurity without accountable governance cannot guarantee legitimacy. Digital Public Infrastructure without technological capability cannot ensure long-term autonomy. Industrial policy without competitive markets may reinforce concentration rather than innovation, while fiscal capacity ultimately determines whether these governance arrangements can be maintained and adapted over time. The effectiveness of each dimension therefore depends upon the others. Hence, data sovereignty is better understood as an institutional system than as a regulatory checklist.

This understanding represents an important departure from much of the existing literature, which frequently approaches data sovereignty through isolated policy instruments or sector-specific governance arrangements. The framework proposed here instead conceives sovereignty as an emergent institutional capacity whose effectiveness depends upon the coherence of constitutional, technological, developmental, economic and governance arrangements operating across the digital stack.

The following subsections examine each constitutive dimension in turn before returning, in Section 3.7, to demonstrate how their interaction must be seen as the basis of an integrated governance framework. The purpose of this progressive presentation is to preserve the analytical specificity of each dimension while showing that data sovereignty ultimately emerges not from any individual component, but from the coherence of the institutional architecture that connects them.

3.1. DATA PROTECTION

The first constitutive dimension of data sovereignty is data protection, which functions as the normative entry point of sovereign digital governance. It provides the constitutional legitimacy upon which every system of data governance ultimately depends, because public authority cannot be exercised legitimately in data-driven societies unless individuals can trust that personal information is

collected, processed, shared and retained in accordance with legality, fairness, transparency, accountability and effective oversight.⁵⁸

Hence, the constitutional significance of data protection extends beyond data privacy. Personal data increasingly mediate access to employment, education, healthcare, financial services, social protection and democratic participation. Decisions concerning eligibility, identity, credit, mobility, public benefits and political expression are increasingly shaped by automated systems operating upon large-scale data processing. Protecting informational self-determination therefore safeguards not only personal autonomy, but also the conditions required for democratic equality, human dignity and the rule of law within increasingly algorithmic societies. As famously stated by art 1 of the 1978 French *Loi Informatique et Libertés*:

“Information technology should be at the service of every citizen. Its development shall take place in the context of international cooperation. It shall not violate human identity, human rights, privacy, or individual or public liberties”

This principle is so fundamental that it has been incorporated as one of the pillars of the proposed Inter-American Convention on Informational Self-Determination, the Processing and Circulation of Personal Data.⁵⁹ However, data protection should not be understood solely as a defensive mechanism designed to constrain public or private power. Well-designed data protection frameworks also perform an enabling function. By establishing predictable legal rules, allocating institutional responsibilities and creating trusted conditions for lawful data sharing, they facilitate innovation, scientific research, efficient public administration and responsible digital transformation.⁶⁰ Data protection therefore creates the legal certainty and institutional trust necessary for legitimate data governance. Data protection therefore creates the foundation of legal certainty and institutional trust necessary for legitimate data governance.

⁵⁸ Brian Nogrères, A. (2022). Principles underpinning privacy and the protection of personal data (UN Doc. A/77/196). United Nations, General Assembly, Brian Nogrères, A. (2023). *Principles of transparency and explainability in the processing of personal data* (UN Doc. A/78/310). United Nations, General Assembly.

⁵⁹ Luca Belli, Ana Brian Nogrères, Jonathan Mendoza Iserte, Pablo Andrés Palazzi and Nelson Remolina Angarita, *Transferência Internacional de Dados Pessoais na América Latina: Rumo à Harmonização de Normas* (1st edn, Lumen Juris 2024), Annex A.

⁶⁰ UNCTAD. Cross-border data flows and development: For whom the data flow. Digital Economy Report 2021.

This distinction is particularly important within the framework proposed in this paper. Data governance often requires the lawful circulation of information across institutional boundaries, whether to deliver public services, support DPI, enable interoperable government systems or foster data-driven innovation.⁶¹ For informational self-determination safeguards to be meaningful, data protection also requires solid institutional guarantees. Independent supervisory authorities, enforceable rights, accessible remedies⁶², audit powers and effective sanctions transform abstract principles into practical constraints on governmental and corporate power. Without such mechanisms, data protection risks becoming a formal commitment rather than a durable source of legitimacy within the broader architecture of data sovereignty.

For this reason, we argue that data protection constitutes a foundational pillar of data sovereignty rather than its complete expression. It establishes the legitimacy through which authority over personal data may be exercised, but it does not by itself determine who governs critical digital infrastructures, who controls strategic technological capabilities, how interoperable ecosystems are organised or whether states possess the practical capacity to exercise meaningful agency within the digital economy.

Informational self-determination therefore remains indispensable, yet it must be complemented by the additional institutional capacities developed throughout the remainder of this chapter. Data sovereignty begins with rights, but it is realised through governance. Yet rights remain effective only if the infrastructures through which they are exercised remain trustworthy and resilient. Data protection therefore establishes the normative legitimacy of data sovereignty, while cybersecurity preserves the operational conditions under which that legitimacy can be realised.

3.2. CYBERSECURITY AND CYBER-RESILIENCE

The second constitutive dimension is cybersecurity. Traditional discussions of informational self-determination generally assume that legal rights can be meaningfully exercised once appropriate rules governing data processing have been established. Contemporary digital ecosystems challenge this assumption because

⁶¹ Richard Pope, *Platformland: An Anatomy of Next-Generation Public Services* (London: London Publishing Partnership, 2025), 27-45.

⁶² Brian Nougères, A. (2024). *Legal safeguards for personal data protection and privacy in the digital age* (UN Doc. A/HRC/55/46). United Nations, Human Rights Council.

legal rights become ineffective whenever digital infrastructures themselves are compromised.

Recent data protection and cybersecurity frameworks seem to acknowledge this shortcoming, by promoting Security by Design as a core principle – or even “an aspirational mantra”⁶³ – mandating the consideration of the systems’ security needs before they are built and integrating these needs in the systems’ subsequent design and construction.

Cybersecurity therefore transforms sovereignty from a purely legal concept into a question of operational resilience.⁶⁴ A government may adopt exemplary privacy legislation while its databases and digital infrastructure remain vulnerable to ransomware attacks. Citizens may enjoy extensive legal protections concerning their personal information, yet those protections become largely illusory if hostile actors can exfiltrate sensitive information through software vulnerabilities or compromise critical digital infrastructures through cyber operations.⁶⁵

The increasing digitisation of public administration further reinforces this relationship. Tax systems, electoral registers, healthcare records, social protection programmes, payment systems and identity infrastructures now depend upon interconnected digital networks whose disruption may significantly impair the capacity of governments to perform their most basic functions. Consequently, cybersecurity increasingly resembles national defence: it protects not only information but also the institutional continuity of the state itself.⁶⁶

This observation has important conceptual implications. Data sovereignty cannot simply concern control over data; it must also encompass the ability to preserve the integrity, availability and confidentiality of digital ecosystems. Security is therefore not an external prerequisite for sovereignty but one of its constitutive dimensions.

Cybersecurity encompasses the policies, institutions, technologies and operational capabilities required to protect digital assets, systems, networks and the individuals who depend upon them from cyber threats. Increasingly, this concept is complemented by that of cyber-resilience, namely the capacity of digital systems not only to prevent and withstand cyber incidents but also to recover rapidly and

⁶³ Bygrave L.A. Security by Design: Aspirations and Realities in a Regulatory Context. Oslo Law Review. Volume 8, No. 3-2021, p. 126–177.

⁶⁴ Belli, L. et al. Governança e regulação da cibersegurança no Brasil: proteção da infraestrutura crítica, segurança da informação e construção da soberania digital. (Lumen Juris, 2025); Belli, L. et al. Cibersegurança: uma visão sistêmica rumo a uma Proposta de Marco Regulatório para um Brasil Digitalmente soberano. Rio de Janeiro, RJ: FGV Direito Rio, 2023.

⁶⁵ Idem.

⁶⁶ Idem.

continue operating under adverse conditions.⁶⁷ Together, cybersecurity and cyber-resilience provide the institutional conditions necessary for the exercise of sovereignty in the digital environment.

This relationship reflects a broader transformation in the nature of data. Data are no longer merely objects of legal protection; they have become strategic assets underpinning public administration, economic activity, scientific research, critical infrastructure and national security. From the perspective proposed in this paper, data sovereignty therefore extends beyond the governance of data itself to encompass the security of the digital ecosystems that sustain it. Sovereignty today depends not only on the legal authority to regulate data processing but also on the capacity to preserve the confidentiality, integrity and availability (known as the “CIA triad”) of the infrastructures supporting digital society. Data centers, cloud computing platforms, telecommunications networks, submarine cables, and other digital infrastructures alike have become critical, as disruption may compromise the continuity of government, economic stability and democratic institutions.

Hence, this evolution fundamentally changes the relationship between cybersecurity and fundamental rights. Informational self-determination, privacy, freedom of expression, access to public services and democratic participation increasingly depend upon secure digital infrastructures. Indeed, a legal right to data protection provides limited practical protection if personal information can be exfiltrated through cyberattacks, manipulated by malicious actors or rendered inaccessible through ransomware. Cybersecurity should therefore be understood not only as an instrument of national security but also as a positive obligation of the state to create the conditions under which fundamental rights can be effectively exercised.⁶⁸

Importantly, the complementarity between cybersecurity and data governance extends beyond protection. Investments in research, technological development and digital capabilities contribute simultaneously to stronger cybersecurity and more effective regulation. Regulation, technological innovation and operational

⁶⁷ International Organization for Standardization, *ISO 22316:2017 Security and Resilience—Organizational Resilience—Principles and Attributes* (ISO 2017); National Institute of Standards and Technology, *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach* (NIST Special Publication 800-160 vol 2 rev 1, 2021); Richard A Caralli, Julia H Allen, David W White and others, *CERT® Resilience Management Model (CERT®-RMM): A Maturity Model for Managing Operational Resilience* (Version 1.2, CMU/SEI-2016-TR-012, Carnegie Mellon University Software Engineering Institute 2016)

⁶⁸ Belli, L. et al. Governança e regulação da cibersegurança no Brasil: proteção da infraestrutura crítica, segurança da informação e construção da soberania digital. (Lumen Juris, 2025); Belli, L. et al. Cibersegurança: uma visão sistêmica rumo a uma Proposta de Marco Regulatório para um Brasil Digitalmente soberano. Rio de Janeiro, RJ: FGV Direito Rio, 2023.

capability should therefore be understood as mutually reinforcing components of the same governance ecosystem. Accordingly, national cybersecurity strategies should pursue multiple objectives simultaneously. They should strengthen the protection of citizens and public institutions, enhance economic resilience, foster technological capability and support sustainable digital development.⁶⁹ Achieving these objectives requires coordinated action across government, industry, academia and civil society, reflecting the inherently multidisciplinary nature of cybersecurity governance.

Such strategies should encompass several complementary elements, including the establishment of minimum cybersecurity standards; the protection of critical information infrastructure and essential services; the development of national capabilities for monitoring, preventing and responding to cyber incidents; clear institutional responsibilities for regulatory oversight and enforcement; mechanisms for information sharing and operational coordination among public authorities and private operators; investment in cybersecurity research and workforce development; and support for trusted digital technologies capable of reducing strategic vulnerabilities while remaining interoperable with international systems.⁷⁰

The growing strategic importance of cybersecurity also reinforces the need to reduce excessive technological dependency in critical sectors. While no country can realistically achieve complete technological autonomy, excessive reliance on external digital infrastructures, cloud services or software ecosystems may expose essential public functions to strategic vulnerabilities beyond the direct control of national authorities. Building cybersecurity capacity therefore requires not only technical expertise but also investments in trusted digital infrastructure, resilient supply chains and diversified technological ecosystems capable of supporting the continuity of essential public services.

At the same time, cybersecurity illustrates why data sovereignty cannot be pursued through isolation. Digital ecosystems are inherently interconnected, and cyber threats routinely transcend national borders. Vulnerabilities affecting software, cloud services, telecommunications infrastructure or supply chains frequently generate cascading effects across multiple jurisdictions. Effective cybersecurity therefore depends upon international cooperation in areas such as cybercrime, incident response, threat intelligence, technical standards and the protection of critical infrastructure.

Ultimately, cybersecurity and cyber-resilience are not simply supporting policies within the broader framework of data sovereignty. They constitute indispensable

⁶⁹ Idem.

⁷⁰ Belli L. and others, *Soberania Digital e Inteligência Artificial no Brasil: Rumo à autonomia tecnológica* (Lumen-Juris 2026).

governance capacities without which none of the other dimensions of data sovereignty can be effectively realized. Accordingly, cybersecurity expands informational self-determination from protecting individual autonomy to safeguarding the institutional conditions under which autonomy can be exercised. Security alone, however, does not determine how digital public authority is exercised. Once resilient infrastructures exist, the next question concerns how they should be organised to deliver public functions and coordinate data governance. This is the ideal role of Digital Public Infrastructure.

3.3. DIGITAL PUBLIC INFRASTRUCTURE

If cybersecurity preserves the integrity, availability and resilience of digital ecosystems, Digital Public Infrastructure determines whether those secure ecosystems can be used to operationalize public authority, deliver rights and services, and coordinate data governance in practice. If cybersecurity preserves the integrity, availability and resilience of digital ecosystems, Digital Public Infrastructure (DPI) determines whether those secure ecosystems can be used to operationalize public authority, deliver rights and services, and coordinate data governance in practice. Security protects the conditions under which autonomy can be exercised; DPI provides the institutional and technological architecture through which that autonomy becomes administratively effective, socially accessible and democratically accountable.

DPI contributes to data sovereignty because it aims at operationalising data governance through systems that remain accountable, interoperable, secure and democratically controllable. One of the defining features of contemporary digital governance is that public authority increasingly depends not only upon legal rules, but also upon the infrastructures through which those rules become effective. Data protection legislation, administrative law, consumer protection, competition law, cybersecurity regulation and sectoral governance remain indispensable foundations of the digital state. Their practical effectiveness, however, depends upon the design and governance of the systems through which identities are established, transactions are executed, information is exchanged and access to public services is organized.

DPI should therefore be understood as more than a collection of digital technologies, applications or government platforms. Recent policy and academic work describes DPI as shared, foundational and interoperable capabilities capable of supporting multiple public and private services at societal scale. This paper builds upon that understanding while advancing a broader institutional proposition: DPI is public not merely because it is publicly accessible or financed, but because it creates the

technological and institutional conditions through which public authority can be exercised, coordinated, constrained and made accountable within digital services.⁷¹

This interpretation clarifies what makes such infrastructure genuinely public. Digital infrastructures are not neutral arrangements: their design and governance embody directions, distribute value and shape relationships among public institutions, private actors and society.⁷² The public character of DPI cannot therefore be inferred solely from government ownership, public financing or universal availability. It depends upon whether the infrastructure pursues democratically defined public purposes, generates broadly shared public value and remains accountable to the institutions and communities affected by it.⁷³

Publicness is therefore an institutional quality rather than a simple property classification. A government-owned platform may undermine sovereignty if it relies upon opaque proprietary components, irreplaceable vendors or contractual arrangements that prevent auditing, modification or migration. Conversely, privately developed or open-source components may contribute to public infrastructure where they remain interoperable, contestable, portable and subject to effective public governance. The relevant questions are not limited to who owns the servers or software, but they include who defines the purposes of the infrastructure, who controls standards and interfaces, who authorizes access, who bears responsibility for failure and whether democratic institutions retain the capacity to alter its technological direction.

DPI may accordingly be described as constitutional architecture in a functional sense. It is not constitutional because it replaces constitutional law, nor because technical design can become the autonomous source of legitimacy. Rather, it is constitutional because it structures how legally constituted authority is implemented and experienced in practice. This insight extends Lessig's proposition that architecture constitutes a modality of regulation, while remaining consistent with Hildebrandt's warning that technological design cannot substitute for the rule

⁷¹ Ole Hanseth and Kalle Lyytinen, 'Design Theory for Dynamic Complexity in Information Infrastructures' (2010) *Journal of Information Technology*; OECD, *Digital Public Infrastructure for Digital Governments* (OECD Public Governance Policy Papers No 68, OECD Publishing 2024) ; David Eaves and Krisstina Rao, *Digital Public Infrastructure: A Framework for Conceptualisation and Measurement* (UCL Institute for Innovation and Public Purpose Working Paper 2025).

⁷² Brett Frischmann, *Infrastructure: The Social Value of Shared Resources* (Oxford University Press 2012).

⁷³ Idem.

of law.⁷⁴ DPI should make legal principles technically effective while preserving institutional checks, interpretative openness, due process, judicial review and democratic accountability.

The institutional importance of DPI lies in the transition from isolated applications to reusable public capabilities. Governments have traditionally developed digital services in organizational silos, repeatedly reconstructing functions such as identity verification, authentication, payments, notifications, document exchange and records management. The Government as a Platform literature⁷⁵ shows how common components, data and interfaces can reduce duplication and support service development across the public sector. DPI builds upon this platform logic but extends beyond administrative efficiency: shared identity, payment, data exchange, credential and trust capabilities shape the distribution of authority, responsibility and access across society.

Concrete examples illustrate this constitutional function. Digital identity systems influence who can be recognized by public institutions, which attributes individuals must disclose, how rights and entitlements are proven and whether errors can be challenged. Payment infrastructures such as Brazil's Pix or India's UPI affect financial inclusion, public transfers, competition and the relationship between public authority and regulated financial actors. Trusted data exchange frameworks such as Estonia's X-Road, and emerging digital credential systems such as the EU Digital Identity Wallet, similarly enable authoritative assertions to circulate and be recognized across institutional boundaries. Their significance lies not only in convenience or efficiency, but in the institutional conditions they create for recognition, participation and accountability.

These shared capabilities expand what Mann describes as the infrastructural power of the state: the capacity of public institutions to coordinate social and administrative activity through durable arrangements extending across society.⁷⁶ Hence, DPI can increase the ability of governments to identify needs, deliver

⁷⁴ Lessig, L. 'The Law of the Horse: What Cyberlaw Might Teach' (1999) 113(2) Harvard Law Review 501;

Lessig, L. Code: Version 2.0 (Basic Books 2006); Mireille Hildebrandt, 'Algorithmic Regulation and the Rule of Law' (2018) 376(2128) *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 20170355

⁷⁵ Tim O'Reilly, 'Government as a Platform' in Daniel Lathrop and Laurel Ruma (eds), *Open Government: Collaboration, Transparency, and Participation in Practice* (O'Reilly Media 2010) 11–40; Helen Margetts and André Naumann, *Government as a Platform: What Can Estonia Show the World?* (Oxford Internet Institute, University of Oxford 2017).

⁷⁶ Mann, M. (1984). The autonomous power of the state: Its origins, mechanisms and results. *European Journal of Sociology / Archives Européennes de Sociologie*, 25(2), 185–213

benefits, verify obligations and coordinate public action. Yet infrastructural power is normatively ambivalent. The same capacity that enables more effective service delivery may also enable surveillance, exclusion, automated control or the rapid propagation of administrative errors. The constitutional question is therefore not whether the state should possess infrastructural capacity, but how that capacity is distributed, governed and constrained.

A federated and polycentric model offers one means of reconciling infrastructural capacity with distributed authority. Drawing upon Ostrom's work⁷⁷, DPI can be understood as an arrangement in which multiple autonomous institutions exercise responsibility within their respective domains while cooperating under shared rules. Civil registries, tax administrations, health authorities, educational institutions, central banks and other public bodies may remain authoritative for the records and functions legally entrusted to them, while shared infrastructure enables cooperation without transferring all data or decision-making authority to a single central platform. Such federation, however, requires common standards, semantic definitions, assurance frameworks, identity and access controls, audit rules and processes for resolving inconsistencies.

Data governance constitutes the constitutional layer that defines institutional authority, lawful purposes for data processing, conditions for access and reuse, quality standards and mechanisms for oversight and redress. DPI operationalizes these legal and institutional arrangements through technological architecture but does not itself create legal authority. Indeed, trusted data collaboration among public institutions, private actors and civil society depends upon clearly defined purposes, differentiated access and robust accountability mechanisms.

Because DPI mediates the exercise of public authority, constitutional safeguards must be embedded by design. Principles such as purpose limitation, proportionality and data minimization should govern data exchange, while technologies including selective disclosure, verifiable credentials, role-based access controls and tamper-evident audit logs can strengthen privacy and accountability.⁷⁸ Human oversight, accessible correction procedures, effective remedies and inclusive service delivery

⁷⁷ E.g., Ostrom, Elinor. "Beyond Markets and States: Polycentric Governance of Complex Economic Systems." *American Economic Review* 100, no. 3 (2010): 641-672. Ostrom, Elinor. "Polycentric Systems for Coping with Collective Action and Global Environmental Change." *Global Environmental Change* 20, no. 4 (2010): 550-557. Ostrom, Elinor. *Understanding Institutional Diversity*. Princeton: Princeton University Press, 2005.

⁷⁸ Hannah Draper, and others. *A Consumer-centric Approach to Digital Public Infrastructure for Sustainable Financial Inclusion* (T20 Brasil Policy Brief, Task Force 5, 2024)

– including meaningful non-digital alternatives – remain essential to preserving due process and equal access.⁷⁹

At the same time, poorly governed DPI may generate new risks.⁸⁰ Excessive centralization can facilitate surveillance, function creep, automated exclusion and systemic failures, while interoperability may expand access to sensitive data beyond legitimate purposes. Accordingly, data sovereignty requires the institutional capacity to audit, modify and replace digital infrastructure. Properly governed, DPI becomes a constitutional component of data sovereignty: an interoperable, secure and accountable institutional architecture that strengthens public authority while preserving institutional autonomy, democratic accountability and fundamental rights. Its long-term sustainability, however, ultimately depends upon domestic technological and industrial capabilities capable of developing, maintaining and continuously improving essential digital infrastructures.

3.4. INDUSTRIAL DEVELOPMENT AND TECHNOLOGICAL CAPABILITY

Industrial development constitutes an indispensable dimension of data sovereignty because governance ultimately depends not only on legal authority, but also on the productive capabilities that enable societies to shape the technologies through which data are generated, processed and exchanged. While data sovereignty is often discussed in terms of jurisdiction, regulatory competence or control over information flows, these legal and institutional dimensions cannot be fully realised in the absence of domestic capabilities to develop, adapt, maintain and govern digital infrastructures.⁸¹ Sovereignty therefore requires more than the authority to regulate technological change; it requires the capacity to participate meaningfully in its production and direction.

This understanding reflects a broader evolution in industrial policy itself. Contemporary industrial policy no longer focuses primarily on protecting domestic industries or correcting isolated market failures. Rather, it increasingly seeks to shape technological trajectories by coordinating public and private investment around strategically defined missions.⁸² Likewise, Rodrik emphasises that modern industrial policy should be understood as a process of institutional discovery

⁷⁹ Brian Nougères, A. (2024). *Legal safeguards for personal data protection and privacy in the digital age* (UN Doc. A/HRC/55/46). United Nations, Human Rights Council.

⁸⁰ Idem.

⁸¹ Belli L. and others, *Soberania Digital e Inteligência Artificial no Brasil: Rumo à autonomia tecnológica* (Lumen-Juris 2026).

⁸² Mazzucato, Mariana. *The Entrepreneurial State: Debunking Public vs. Private Sector Myths*. London: Anthem Press, 2013. Revised edition, PublicAffairs, 2015.

through which states and firms jointly develop productive capabilities under conditions of structural transformation⁸³. From this perspective, industrial policy is not simply an instrument for promoting economic growth, but a mechanism through which governments expand the governance capacity required to pursue collectively determined public objectives.

Applied to the digital economy, this shift has profound implications. Productive capability is no longer measured primarily by manufacturing capacity or ownership of physical assets. Instead, it increasingly depends upon the ability to design, deploy and continuously improve complex socio-technical systems, including cloud infrastructures, advanced semiconductor supply chains, cybersecurity capabilities, AI systems, and DPIs.⁸⁴ Sovereignty therefore depends less on technological self-sufficiency than on the institutional capacity to shape the evolution of these interconnected technological systems.

This distinction is particularly important because digital transformation unfolds through successive technological paradigms rather than isolated innovations. Indeed, the capacity to sustain development depends not merely upon the invention of new technologies but upon their widespread diffusion throughout productive systems and institutions⁸⁵. Countries that successfully develop governance arrangements capable of absorbing and adapting technological change often derive greater long-term benefits than those that simply generate frontier innovations. From the perspective of data sovereignty, this implies that governance capacity depends upon both creating new technologies and embedding them within resilient institutional, regulatory and economic structures.

Innovation itself has also become increasingly ecosystemic.⁸⁶ Rather than occurring within isolated firms, innovation now emerges from interactions among technology developers, infrastructure providers, public institutions, research organisations and complementary service providers. Gawer has shown that digital platforms increasingly function as innovation ecosystems whose governance shapes the opportunities available to participants throughout the wider economy⁸⁷. This

⁸³ Rodrik, Dani. "Industrial Policy for the Twenty-First Century." Working paper prepared for UNIDO, September 2004.

⁸⁴ Belli, L. and Bhinder, A. Cooperative Digital Sovereignty and Artificial Intelligence Promoting Resilience, Strategic Openness, and Self-Determination. (Digital Cooperation Organization, 2026).

⁸⁵ Perez, Carlota. Technological Revolutions and Financial Capital: The Dynamics of Bubbles and Golden Ages. Cheltenham: Edward Elgar, 2002.

⁸⁶ Nicolo Zingales and Paula Farani de Azevedo (eds), *A Aplicação do Direito Antitruste em Ecossistemas Digitais: Desafios e Propostas* (FGV Direito Rio 2022)

⁸⁷ Gawer, Annabelle. "Digital Platforms' Boundaries: The Interplay of Firm Scope, Platform Sides, and Digital Interfaces." *Long Range Planning* 54, no. 5 (2021): 102045. See also Gawer, Annabelle.

observation significantly expands the meaning of industrial policy. Public intervention is no longer limited to supporting individual firms or sectors; it increasingly concerns the governance of the ecosystems through which innovation is generated, coordinated and diffused.

Viewed through this lens, industrial policy contributes to data sovereignty by strengthening what this paper conceptualises as governance capacity. Investments in research and development, advanced digital skills, cybersecurity, trusted computing infrastructure, open technological standards and interoperable public infrastructures expand the range of institutional options available to governments, firms and civil society. Sovereignty therefore becomes less a question of ownership over digital assets than of preserving the collective capacity to shape technological development according to democratically determined priorities.⁸⁸

This perspective also helps explain why AI has become a central concern of contemporary industrial policy. AI capability should not be equated solely with the ability to develop frontier foundation models. Rather, meaningful participation in the emerging AI economy increasingly depends upon the capacity to access and muster Key AI Sovereignty Enablers such as computing infrastructure, evaluation capacity, trustworthy datasets, advanced digital skills and the institutional capability to deploy AI systems responsibly across multiple sectors.⁸⁹

Digital production increasingly occurs within ecosystems whose operation cannot be reduced either to decentralised market coordination or to hierarchical state direction. Ecosystems organise complementarities among infrastructure providers, application developers, data holders, public institutions and users, while their governing actors determine the conditions of access, interoperability and value creation. Data collaboratives, for instance, should be treated simply as mechanisms for releasing additional datasets. Their significance lies in their capacity to structure cooperation among actors possessing different resources, mandates and responsibilities, subject to rules governing access, purpose, accountability and the allocation of benefits and risks⁹⁰. In this respect, they illustrate how productive

“Bridging Differing Perspectives on Technological Platforms: Toward an Integrative Framework.” *Research Policy* 43, no. 7 (2014): 1239-1249.

⁸⁸ Belli, L. and Bhinder, A. *Cooperative Digital Sovereignty and Artificial Intelligence Promoting Resilience, Strategic Openness, and Self-Determination*. (Digital Cooperation Organization, 2026).

⁸⁹ Belli, L. “To Get Its AI Foothold, Brazil Needs to Apply the Key AI Sovereignty Enablers (KASE).” In Feldstein S. (ed.) *New Digital Dilemmas: Resisting Autocrats, Navigating Geopolitics, Confronting Platforms*. (Carnegie Endowment for International Peace, 2023) ; Belli L. and others, *Soberania Digital e Inteligência Artificial no Brasil: Rumo à autonomia tecnológica* (Lumen-Juris 2026).

⁹⁰ Zingales, Nicolo. “Data Collaboratives, Competition Law and the Governance of EU Data Spaces.” In *Research Handbook on the Law and Economics of Competition Enforcement*, edited by Ioannis Kokkoris. Cheltenham: Edward Elgar, 2022.

capacity may be supported by institutional arrangements that are neither exclusively state-directed nor purely proprietary.

These arrangements also reveal why digital industrial policy should be understood in polycentric rather than exclusively centralised terms. Ostrom's account of polycentric governance emphasises that complex collective problems may be addressed through multiple, partially autonomous centres of decision-making operating under overlapping rules and mechanisms of coordination.⁹¹ Applied to digital development, this suggests that productive capability need not be concentrated within a single ministry, public enterprise or nationally favoured firm. It may instead emerge from the coordinated activity of research institutions, public authorities, infrastructure operators, private enterprises, open-source communities and civil-society organisations. The relevant sovereign capacity lies in maintaining the institutional conditions under which these actors can cooperate, experiment and remain mutually accountable, while preventing any single centre of power from becoming structurally indispensable.

At the same time, industrial policy needs to be seen as an essential complement of competition policy: while the former primarily enhances technological autonomy by expanding domestic capabilities, the latter primarily enhances resilience by preventing excessive dependence upon individual firms, technologies or infrastructures.

Ultimately, data sovereignty requires moving beyond a regulatory conception of governance towards a productive conception. States must regulate digital technologies, but they must also possess the capacity to produce, adapt and continuously improve them. Governance and productive capability become mutually reinforcing dimensions of sovereignty. Yet productive capability alone cannot guarantee sovereignty. If industrial policy merely replaces foreign concentration with domestic concentration, technological dependence may simply change its source. The benefits of industrial development therefore depend upon competitive market structures capable of preserving contestability, innovation and technological plurality.

3.5. COMPETITION AND INNOVATION

If industrial policy expands the range of technological and productive options available to a society, competition policy helps preserve those options by preventing control over digital ecosystems from becoming irreversibly concentrated. The two dimensions are therefore complementary. Industrial policy without competition policy may create capabilities while allowing their appropriation by a limited

⁹¹ Ostrom, Elinor. "Polycentric Systems for Coping with Collective Action and Global Environmental Change." *Global Environmental Change* 20, no. 4 (2010): 550-557.

number of firms. Competition policy without industrial policy may preserve formal market openness while failing to generate the infrastructures, skills and organisations needed for meaningful participation. Data sovereignty requires both: the capacity to develop technological alternatives and institutional arrangements that keep those alternatives viable.

The relevance of competition policy to data sovereignty cannot be captured fully by conventional concerns with prices, output or short-term consumer welfare. Digital markets are frequently characterised by network effects, economies of scale and scope, access to large volumes of data, high switching costs and complementarities among services.⁹² These features may permit a firm that controls one strategic layer of an ecosystem to influence entry and innovation across several adjacent layers. The resulting power is not merely economic. It includes the capacity to determine technical interfaces, conditions of access, defaults, data-sharing practices, developer rules and interoperability standards. Concentration may therefore transfer decisions that shape the future organisation of digital markets from public institutions and dispersed market participants to privately governed infrastructures.

Digital ecosystems make this problem particularly visible.⁹³ They consist not simply of collections of related products but of interdependent services, technologies and actors organised around common infrastructures and governed through interfaces, standards and contractual rules. Competition consequently takes place both within ecosystems and between them. A platform may face competition at one layer while retaining decisive influence over the infrastructure or gateway upon which competitors at another layer depend⁹⁴

This ecosystemic perspective also requires a more precise understanding of innovation. Innovation does not occur solely through rivalry among vertically integrated firms producing substitutable products. It often depends upon complementarities among infrastructure providers, application developers, data holders and users. Governance decisions concerning access to interfaces, portability, interoperability and data may therefore determine who can innovate, on what terms and at which technological layer. The relevant objective is not to maximise the number of competitors in the abstract, but to preserve an institutional

⁹² Nicolò Zingales and Paula Farani de Azevedo (eds), *A Aplicação do Direito Antitruste em Ecosistemas Digitais: Desafios e Propostas* (FGV Direito Rio 2022)

⁹³ Idem.

⁹⁴ See, for instance, Jacobides, Michael G., and Ioannis Lianos. "Ecosystems and Competition Law in Theory and Practice." *Industrial and Corporate Change* 30, no. 5 (2021): 1199–1229.; Zingales, Nicolò, and Bruno Polonio Renzetti. "Digital Platform Ecosystems and Conglomerate Mergers: A Review of the Brazilian Experience." *World Competition* 45, no. 4 (2022): 473–514.

environment in which alternative services, business models and technological trajectories can emerge.

Competition policy contributes to sovereignty by preserving this governance optionality. Contestability ensures that governments, firms and users are not confined permanently to the standards, contractual arrangements or technological direction selected by a dominant undertaking. The possibility of switching providers, combining services, accessing essential interfaces or developing interoperable alternatives preserves the capacity of public and private actors to revise technological choices over time. In this sense, competition protects not only present rivalry but also future institutional choice.

This claim does not imply that every form of concentration is incompatible with innovation. Significant economies of scale may be necessary for cloud computing, semiconductor fabrication, payment infrastructure and frontier artificial intelligence. Large firms may possess resources that enable costly and risky forms of research and development. The sovereignty concern arises when scale becomes structural indispensability: when governments, businesses or users cannot realistically migrate, interoperate or support alternatives without prohibitive cost or disruption.⁹⁵ Competition policy should therefore focus not only on the size of firms, but on whether ecosystem governance preserves viable exit, entry, substitution and innovation pathways.

Data-related conduct offers a particularly important illustration. Data may be used to improve products and coordinate services, but they may also be deployed to exclude rivals, exploit dependent users, discriminate among business partners or extend power into adjacent activities.. The legal significance of a practice depends upon the position occupied by the undertaking, the function of the data within the relevant ecosystem, the relationship between the parties and the exclusionary or exploitative effects produced. This differentiated approach is compatible with the framework developed here: data sovereignty is undermined not by data concentration as such, but by uses of data that foreclose institutional alternatives, entrench dependency or prevent affected actors from participating on fair terms.

These concerns explain the growing movement from exclusively ex post enforcement toward more explicit forms of ex ante digital market governance. The EU Commission's report by Crémer, de Montjoye and Schweitzer⁹⁶ argued that the characteristics of the digital economy required the adaptation of competition-law

⁹⁵ Belli L. and others, *Soberania Digital e Inteligência Artificial no Brasil: Rumo à autonomia tecnológica* (Lumen-Juris 2026).

⁹⁶ Crémer, Jacques, Yves-Alexandre de Montjoye and Heike Schweitzer. *Competition Policy for the Digital Era*. European Commission, 2019

concepts, methodologies and remedies, particularly in relation to platforms, data and innovation. The Furman Review⁹⁷ similarly proposed a pro-competitive regulatory regime centred on firms possessing strategic market status, accompanied by rules concerning interoperability, data mobility and market-opening measures. These initiatives helped establish the intellectual foundations for contemporary regimes such as the European Union's Digital Markets Act and the United Kingdom's digital markets framework.

The significance of this regulatory evolution lies not merely in the introduction of additional obligations for large firms. It reflects a shift in the object of competition governance. Rather than intervening only after a clearly defined infringement within a particular market, digital regulation increasingly seeks to maintain the institutional conditions of contestability across ecosystems. Obligations concerning interoperability, portability, access to data, self-preferencing, tying and the governance of application stores or operating systems are directed at the architecture through which economic coordination occurs. Competition law and regulation thus become mechanisms for governing infrastructural power.

Digital Public Infrastructure can reinforce these objectives, but only under specific governance conditions. By transforming identity, payment or data-exchange functions into shared and interoperable capabilities, DPI may reduce the need for each market participant to reproduce foundational infrastructure. Modular infrastructures separate foundational layers from competitive application layers, facilitating distributed innovation while reducing lock-in⁹⁸. This can lower entry costs and permit competition at the level of applications and complementary services. Pix and UPI illustrate how common payment rails may enable banks and fintech firms to innovate within a shared architecture rather than compete through closed proprietary networks.

However, the public character of infrastructure does not automatically guarantee competitive outcomes. DPI may itself reinforce market concentration if access conditions are discriminatory, technical standards are controlled by incumbents, procurement practices create dependence on irreplaceable vendors, or interoperability is only nominal. Competition-enhancing DPI therefore requires open standards, documented interfaces, portability, modular design, transparent governance and proportionate access conditions that enable meaningful participation and technological substitution.⁹⁹

⁹⁷ Digital Competition Expert Panel. *Unlocking Digital Competition*. HM Treasury, 2019, commonly referred to as the Furman Review

⁹⁸ Baldwin, Carliss Y., and Kim B. Clark. *Design Rules, Volume 1: The Power of Modularity*. MIT Press, 2000.

⁹⁹ Doctorow, C. (2021). *How to destroy surveillance capitalism*. Medium Editions.

Public procurement constitutes a critical instrument in this regard. As major purchasers of cloud services, software, cybersecurity and artificial intelligence, governments can shape market structure through requirements for interoperability, auditability, open standards, data portability and exit strategies, thereby strengthening both competition and public autonomy.

Similarly, data collaboratives can expand access to valuable datasets and foster innovation across public, private and research sectors, provided they operate under clear governance arrangements. Their contribution to competitive digital ecosystems depends upon transparent participation rules, equitable access, appropriate safeguards and accountability mechanisms that prevent the emergence of new gatekeepers.¹⁰⁰

Ultimately, competition governance in digital ecosystems requires a polycentric approach involving competition authorities, data protection regulators, cybersecurity agencies, procurement bodies and standards organisations. From the perspective of data sovereignty, competition policy performs three essential functions: preventing the concentration of infrastructural power, preserving technological plurality through interoperability and substitution, and enabling a broader range of actors to participate in digital innovation. Competition is therefore not merely an economic objective but a constitutional condition for maintaining collective control over digital transformation.

Yet competitive ecosystems cannot be sustained by regulatory intervention alone. Competition authorities, public infrastructures, research systems and innovation policies require durable financial resources, while the value generated within digital ecosystems remains unevenly distributed. The preservation of governance optionality therefore leads directly to the sixth dimension of data sovereignty: the fiscal capacity to maintain these institutional arrangements and ensure that data-driven economic activity contributes to broader public value. Competition preserves not only current rivalry but also future innovation opportunities by preventing irreversible technological lock-in¹⁰¹.

3.6. FISCAL JUSTICE AND DATA EQUITY

Perhaps the least explored dimension of data sovereignty concerns taxation. Yet fiscal capacity has historically constituted one of the defining attributes of sovereign

¹⁰⁰ Zingales, Nicolo. "Data Collaboratives, Competition Law and the Governance of EU Data Spaces." In *Research Handbook on the Law and Economics of Competition Enforcement*, edited by Ioannis Kokkoris. Cheltenham: Edward Elgar, 2022.

¹⁰¹ Federico, Giulio, Fiona Scott Morton and Carl Shapiro. "Antitrust and Innovation: Welcoming and Protecting Disruption." *Innovation Policy and the Economy* 20 (2020): 125–190. (Originally NBER Working Paper No. 26005, 2019.)

authority. From the emergence of the modern state onwards, the ability to raise revenue has enabled governments to provide public goods, maintain institutions, invest in infrastructure and pursue developmental objectives. Digital transformation has not diminished the importance of taxation; rather, it has fundamentally altered the conditions under which value is created and distributed.

Data-intensive business models generate extraordinary economic value through activities that frequently transcend traditional concepts of physical presence or territorial establishment. Digital platforms may derive substantial revenues from users located within a jurisdiction while maintaining limited taxable presence under conventional international tax rules. Similarly, data generated collectively by societies contribute significantly to the development of AI systems, targeted advertising, algorithmic optimisation and numerous other commercially valuable applications whose economic returns remain highly concentrated.

These developments raise questions extending beyond tax administration. They concern the distribution of value generated by the digital economy itself.¹⁰² If data are increasingly recognised as strategic economic resources, then the benefits derived from their exploitation should contribute to broader social welfare rather than accruing exclusively to those possessing the greatest technological capability or market power. Fiscal policy therefore becomes an instrument through which societies can ensure that digital transformation supports inclusive development rather than reinforcing existing inequalities.

Recent international initiatives led by the OECD/G20 Inclusive Framework have sought to adapt international taxation to the challenges posed by highly digitalised business models.¹⁰³ Although these reforms represent important progress, they primarily address questions concerning allocation of taxing rights and minimum corporate taxation. The broader relationship between taxation and data governance remains comparatively underdeveloped.

This paper therefore proposes understanding taxation as an integral dimension of data sovereignty rather than as a separate area of fiscal policy. First, taxation provides governments with the resources necessary to invest in cybersecurity, Digital Public Infrastructure, digital education, research and innovation. Without adequate fiscal capacity, many of the other dimensions of sovereignty become difficult to sustain over time.

¹⁰² Belli L., Fossati G. McClaskey L. and Zingales, N. *Proteção, Tributação e Equidade de Dados: Equilibrando Valores, Riscos e Obrigações na Economia Digital*. (Lumen Juris 2026)

¹⁰³ Organisation for Economic Co-operation and Development (OECD), *Addressing the Tax Challenges of the Digital Economy, Action 1 – 2015 Final Report* (OECD/G20 Base Erosion and Profit Shifting Project, OECD Publishing 2015) ; OECD, *Tax Challenges Arising from Digitalisation – Report on Pillar One Blueprint: Inclusive Framework on BEPS* (OECD/G20 Base Erosion and Profit Shifting Project, OECD Publishing 2020)

Second, taxation contributes to correcting distributive asymmetries generated by highly concentrated digital markets. Public investment financed through revenues generated by digital economic activity can support broader participation in digital transformation, thereby strengthening both social cohesion and economic resilience.

Third, fiscal policy can encourage responsible data governance through appropriately designed incentives. Tax measures supporting investment in cybersecurity, trusted digital infrastructures, open technologies or domestic innovation ecosystems illustrate how fiscal instruments may reinforce broader governance objectives.

Finally, taxation should be understood within the broader concept of data equity.¹⁰⁴ Data are rarely created by isolated individuals acting independently. They emerge through complex interactions involving citizens, businesses, public institutions and digital infrastructures. Their economic value is therefore inherently relational and collective. Data equity recognises that societies contributing to the creation of this value possess legitimate claims concerning its distribution and public utilisation.

This does not imply assigning proprietary ownership rights over all data generated within a jurisdiction. Rather, it recognises that governments have legitimate authority to design fiscal and regulatory frameworks ensuring that digital transformation contributes to inclusive economic development, social investment and public welfare. Accordingly, fiscal justice constitutes an essential constitutive dimension of data sovereignty, considering that without sustainable public resources, the institutional capacities required for meaningful sovereignty cannot be maintained. Just as taxation historically enabled the construction of roads, schools, courts and public health systems, it increasingly finances the digital infrastructures upon which contemporary sovereignty depends.

3.7. DATA SOVEREIGNTY AS AN INTEGRATED GOVERNANCE FRAMEWORK

The preceding analysis shows that data sovereignty cannot be reduced to any single legal doctrine, technological asset or policy instrument. Data sovereignty is better understood as an emergent institutional capacity produced by the interaction of mutually reinforcing legal, technological, economic and administrative arrangements.

The six dimensions examined in this section each perform a distinct governance function. Data protection supplies the rights-based foundation of legitimacy by safeguarding informational self-determination and fundamental freedoms.

¹⁰⁴ Belli L., Fossati G. McClaskey L. and Zingales, N. Proteção, Tributação e Equidade de Dados: Equilibrando Valores, Riscos e Obrigações na Economia Digital. (Lumen Juris 2026)

Cybersecurity protects the integrity, availability and resilience of the digital systems upon which public authority increasingly depends. Digital Public Infrastructure provides shared institutional capabilities through which rights, services and public functions can be operationalized at scale. Industrial development and technological capability sustain the productive base required to design, maintain and adapt strategic digital infrastructures. Competition and innovation preserve openness, contestability and technological plurality. Fiscal justice and data equity provide the resources and distributive mechanisms needed to ensure that digital transformation generates public value rather than merely private accumulation.

A governance mechanism aimed at building data sovereignty should act as the coordinating layer across these dimensions rather than as an additional constitutive dimension. It allocates authority, responsibility, access, accountability and redress in relation to data and their legitimate uses. In doing so, it connects rights, infrastructure, security, markets, industrial policy and fiscal capacity within a coherent institutional architecture. Without such coordination, the six dimensions risk remaining fragmented: data protection may establish formal rights without effective enforcement; cybersecurity may protect systems without democratic accountability; DPI may enable service delivery without adequate safeguards; industrial policy may build capacity without inclusion; competition policy may open markets without ensuring public value; and fiscal policy may raise revenue without strengthening the institutional foundations of sovereignty.

This integrated conception provides the analytical payoff of the framework. It explains why partial approaches to digital governance often fail to produce meaningful sovereignty. Data sovereignty is therefore not located in a dataset, a server, a platform, a statute or a public agency. It is produced through the relationships among institutions, infrastructures, rules and capabilities that allow democratic authorities to govern digital transformation legitimately, effectively and accountably. This also means that sovereignty is dynamic rather than static and, therefore, any sovereignty oriented governance needs to be underpinned by solid situational awareness mechanisms, able to identify threats, assess risks and support timely, informed decision-making.¹⁰⁵ It must be continuously maintained as technologies, markets, risks and geopolitical conditions evolve. A governance architecture that is sovereign at one moment may become dependent or fragile if it cannot adapt to new technological standards, security threats, market structures or forms of value extraction.

This perspective also clarifies why debates on data sovereignty often appear fragmented or contradictory. Different epistemic communities emphasize different

¹⁰⁵ Belli L. and others, *Soberania Digital e Inteligência Artificial no Brasil: Rumo à autonomia tecnológica* (Lumen-Juris 2026).

parts of the same institutional problem. Constitutional scholars focus on rights, dignity and autonomy. Cybersecurity experts prioritize resilience and critical infrastructure protection. Public administration scholars emphasize state capacity and service delivery. Economists examine innovation, concentration and value distribution. Development scholars highlight dependency, inequality and technological capability. Each perspective identifies a real component of sovereignty, but none alone captures the full governance challenge.

Understanding data sovereignty as an integrated governance framework reconciles these perspectives by locating them within a common institutional project. The central objective is to preserve the capacity of individuals, societies and states to shape the legal, technical and economic conditions under which data and digital infrastructures are governed. That capacity requires rights, but also secure systems; it requires public infrastructure, but also productive capability; it requires markets, but also contestability and fair distribution; it requires domestic authority, but also institutional arrangements capable of managing transnational interdependence.

This final point provides the transition to the next section. If data sovereignty is an integrated capacity rather than territorial control over data alone, the decisive question becomes how that capacity can be exercised within digital ecosystems that are inherently transnational. The answer cannot be technological isolation. It must lie in forms of cooperation that preserve agency while enabling interdependence. Section 4 therefore examines how sovereign digital governance can be pursued through interoperable institutions, shared Digital Public Infrastructure and international cooperation grounded in reciprocity, resilience and the sovereign equality of states.

4. HOW TO BUILD DATA SOVEREIGNTY

The previous section argued that data sovereignty is best understood as an integrated governance capacity rather than as territorial control over data or technological self-sufficiency. It emerges from the interaction of six mutually reinforcing dimensions: data protection, cybersecurity and digital resilience, Digital Public Infrastructure, industrial development and technological capability, competition and innovation, and fiscal justice and data equity. Data sovereignty-oriented governance coordinates these dimensions by allocating authority, responsibility, access, accountability and redress across the institutional architecture through which digital transformation is governed.

The question that follows is how this integrated capacity can be exercised within digital ecosystems that are inherently transnational. This question lies at the centre of contemporary debates on digital sovereignty. As we emphasised, much of the discussion has been framed around technological self-sufficiency, data localization

and domestic control over critical digital assets. These concerns respond to genuine geopolitical, economic and security risks, especially where states depend upon infrastructures, standards or suppliers over which they possess little influence. Yet they also risk presenting sovereignty as a condition that can be achieved primarily through territorial control or technological isolationism.

Such an understanding might be both incorrect and increasingly difficult to reconcile with the architecture of the contemporary digital environment where concentration and distribution coexist. Data routinely traverse multiple jurisdictions within fractions of a second. Cloud infrastructures are geographically distributed. AI models are developed through globally dispersed research communities and trained on internationally sourced datasets. Open-source software underpins much of today's digital infrastructure, while digital trade depends upon interoperable technical standards, trusted credentials and compatible regulatory frameworks. Complete technological autonomy is therefore neither practically achievable nor institutionally desirable.

The challenge confronting states is consequently not how to eliminate interdependence, but how to govern it. Sovereignty is weakened not by cooperation itself, but by forms of dependency that deprive public institutions of meaningful agency over the legal, institutional and technological conditions through which public authority is exercised.¹⁰⁶

This section therefore reimagines data sovereignty as cooperative governance capacity. Sovereignty consists not in preventing data, services or infrastructures from crossing borders, but in preserving the capacity of democratic institutions to determine the conditions under which data, public authority and institutional trust may legitimately circulate across them.

4.1 SOVEREIGN EQUALITY AS THE FOUNDATION

If the previous section established data sovereignty as an integrated institutional capacity, the present subsection asks how that capacity can be exercised among formally equal but materially unequal actors. The answer begins with the principle of sovereign equality. In the digital environment, however, sovereign equality cannot be understood only as equal legal status. It must also be understood in terms

¹⁰⁶ Belli L. and others, *Soberania Digital e Inteligência Artificial no Brasil: Rumo à autonomia tecnológica* (Lumen-Juris 2026); Belli, L. and Bhinder, A. *Cooperative Digital Sovereignty and Artificial Intelligence Promoting Resilience, Strategic Openness, and Self-Determination*. (Digital Cooperation Organization, 2026).

of the institutional agency required to exercise public authority effectively within transnational digital ecosystems.

Article 2(1) of the Charter of the United Nations establishes the sovereign equality of all Member States, affirming that states enjoy equal juridical status irrespective of differences in territory, population, economic power or geopolitical influence. Traditionally, this principle has governed diplomatic relations, treaty-making, jurisdictional competence and the peaceful settlement of disputes. It provides the normative foundation upon which independent political communities cooperate without surrendering their legal autonomy.

Digital transformation reveals the limits of this formal understanding. Legal equality among states does not necessarily translate into an equal capacity to influence the infrastructures, standards and technological systems through which public authority is increasingly exercised..

Sovereign equality in the digital ecosystem should therefore be understood not merely as juridical equality, but as institutional agency: the capacity of public institutions to understand, shape, audit, contest and revise the legal, organisational and technological conditions under which public authority is exercised. This understanding extends rather than replaces the traditional doctrine of sovereign equality. Formal sovereignty remains indispensable, but it becomes insufficient where governments cannot meaningfully influence the standards, infrastructures, contracts or technological capabilities upon which essential public functions depend.¹⁰⁷

This does not require all states to possess identical technological capabilities. Such a standard would be unrealistic and normatively unnecessary. Sovereign equality requires instead that participation in digital ecosystems should not be structured in ways that make some states permanently dependent upon infrastructures, standards, providers or governance arrangements they cannot meaningfully audit, influence or replace. Interdependence is compatible with sovereignty when it preserves choice, reciprocity and institutional adaptability. Dependency emerges when asymmetric relationships allow one actor to constrain another's legitimate public choices.

Conspicuously, these asymmetries are no longer confined to relations among states. Contemporary digital ecosystems are also characterized by unprecedented concentrations of infrastructural power within a relatively small number of private actors. Cloud providers, digital platforms, payment networks, application marketplaces, cybersecurity vendors and developers of foundational AI models

¹⁰⁷ Idem.

increasingly operate infrastructures whose significance extends beyond ordinary commercial activity. Their systems may become functionally public when they mediate access to public services, financial transactions, identity verification, administrative communication or security updates. Decisions concerning interoperability, pricing, security architectures, data portability, access conditions or continuity of service can therefore shape the operational conditions under which public authority is exercised, even without any formal violation of international law.

Applying sovereign equality to digital governance consequently requires more than respect for territorial jurisdiction or the principle of non-intervention. It requires ensuring that states possess meaningful opportunities to participate in shaping the infrastructures, standards, governance frameworks and institutional arrangements that organise the global digital economy. This consideration is particularly important for developing countries, which frequently contribute data, users, innovation and social value to global digital ecosystems while capturing only a limited share of the resulting technological, institutional and economic benefits.¹⁰⁸

Data sovereignty consequently acquires an essential international dimension. It concerns not only the domestic authority of states to regulate data, but also their capacity to participate as institutional equals in shaping the legal, technical and organisational conditions through which digital ecosystems evolve. Sovereignty is therefore strengthened not through technological isolation, but through institutional arrangements that preserve autonomy while enabling cooperation under conditions of reciprocity, resilience and mutual trust. Meaningful autonomy depends less upon eliminating interdependence than upon preserving the capacity to make, contest and revise technological choices over time.

This normative principle, however, cannot operate through legal recognition alone. Sovereign equality supplies the claim that institutions and jurisdictions should cooperate as equals; interoperability supplies the operational means through which that claim becomes administratively, legally and technically practicable. It enables autonomous institutions and jurisdictions to exchange information, recognise credentials, coordinate public services and establish trusted interactions through shared standards and common governance arrangements without requiring institutional uniformity or hierarchical control. Interoperability therefore transforms sovereign equality from a foundational principle of international law

¹⁰⁸ Avila Pinto, R. (2018). Digital sovereignty or digital colonialism? New tensions of privacy, security and national policies. *SUR: International Journal on Human Rights*, 15(27), 15–27; Couldry, N., & Mejias, U. A. (2019). *The costs of connection: How data is colonizing human life and appropriating it for capitalism*. Stanford University Press; Benyera, E. *The Fourth Industrial Revolution and the Recolonisation of Africa: The Coloniality of Data*. (Routledge, 2021);

into an operational principle of digital governance, providing the institutional bridge between legal equality and cooperative sovereignty.

4.2. INTEROPERABILITY AS OPERATIONAL EXPRESSION OF SOVEREIGNTY

If sovereign equality supplies the normative foundation for cooperation in digital environments, interoperability supplies the operational form through which that equality is exercised. Sovereign equality is not self-executing in digital systems. It requires concrete arrangements through which states, public institutions and other legally autonomous actors can cooperate without hierarchy, dependency or loss of constitutional responsibility. Interoperability provides one of the principal mechanisms through which such cooperation becomes possible. It is not merely the technical capacity of systems to exchange and use data, but the governance capacity of autonomous institutions to interact under shared rules while preserving their legal mandates, democratic accountability and decision-making authority.

In this sense, interoperability gives external expression to the integrated conception of data sovereignty developed in Section III. Data protection, cybersecurity, Digital Public Infrastructure, industrial capability, competition and fiscal capacity become mutually reinforcing only when institutions can coordinate across organizational and jurisdictional boundaries under legitimate and accountable conditions. Interoperability is therefore not an additional dimension of sovereignty, but the operational grammar through which the different dimensions of sovereignty can interact without collapsing into a single authority.¹⁰⁹

This understanding requires moving beyond the conventional interpretation of interoperability as a purely technical capability.¹¹⁰ As Lessig argues, architecture itself functions as a form of regulation by shaping the conditions under which behavior becomes possible.¹¹¹ Yet interoperability within public governance extends beyond regulation through technical design. It constitutes part of the

¹⁰⁹ Belli, L. and Zingales, N. (2023). "Interoperability to foster open digital ecosystems in the BRICS countries" (提升互操作性, 构建金砖国家开放数字生态系统). in Chinese Academy of Cyberspace Studies, Xinhua Institute, China Institute of International Studies (中国网络空间研究院, 新华社研究院, 中国国际问题研究院). Shared Vision for the Digital World: Insights from Global Think Tanks on Jointly Building a Community with a Shared Future in Cyberspace (数字世界的共同愿景: 全球智库论携手构建网络空间命运共同体). The Commercial Press (商务印书馆)

¹¹⁰ Ian Brown, *Interoperability as a Tool for Competition Regulation* (OpenForum Academy 2020)

¹¹¹ Lessig, L. Code: Version 2.0 (Basic Books 2006); Mireille Hildebrandt, 'Algorithmic Regulation and the Rule of Law' (2018) 376(2128) *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 20170355

institutional architecture through which public authority is exercised, coordinated and constrained across organizational boundaries. It enables constitutional and administrative principles to become operational without displacing the legal institutions from which those principles derive their legitimacy. In this respect, interoperability should be understood as a mechanism of governance implementation in digital environments.¹¹²

The legitimacy of such implementation depends upon the data governance framework within which interoperable exchanges occur. Decisions regarding who possesses authority over information, the purposes for which information may be processed, the legal basis permitting exchange and the accountability and redress mechanisms applicable to those exchanges cannot be determined by technical compatibility alone. These questions concern the allocation of public authority rather than the movement of data. Governance determines whether an interaction is legitimate; the goal of interoperability should be to determine how that legitimate interaction is implemented across institutional boundaries.

This point connects directly to the role of data protection identified in Section 3.1. Interoperability should aim at facilitating governed interaction among autonomous institutions while preserving legality, fairness, transparency, purpose limitation, proportionality, data minimization, accountability and redress. Helen Nissenbaum's theory of contextual integrity¹¹³ provides an important insight in this regard: the legitimacy of information flows depends not simply upon technical connectivity, but upon the preservation of the contextual norms that govern institutional relationships. Interoperability therefore protects sovereignty only when it sustains, rather than erodes, the legal and institutional context within which data are exchanged.

The significance of interoperability therefore extends beyond the movement of information itself.¹¹⁴ Every interoperable interaction presupposes a relationship of institutional recognition.. Interoperability functions as a governance mechanism through which institutional trust is organized and operationalized. Such trust derives not exclusively from cryptographic assurance or secure communications, but from the legal mandates, governance arrangements and accountability mechanisms that confer legitimacy upon institutional action.

This institutional understanding is consistent with Ostrom's conception of polycentric governance and with the account of data sovereignty as an integrated

¹¹² Ian Brown, *Interoperability as a Tool for Competition Regulation* (OpenForum Academy 2020)

¹¹³ Helen Nissenbaum, 'Privacy as Contextual Integrity' (2004) 79(1) *Washington Law Review* 119–158

¹¹⁴ Ian Brown, *Interoperability as a Tool for Competition Regulation* (OpenForum Academy 2020)

governance framework developed in Section 3.7. Rather than concentrating authority within a single technological platform or administrative hierarchy, interoperable digital ecosystems distribute responsibility among multiple autonomous institutions operating under shared rules. Federated governance arrangements allow authoritative sources to remain within the institutions legally responsible for producing and maintaining them while enabling legitimate cooperation through common standards and trusted interfaces. Sovereignty is therefore preserved not through centralization but through coordinated institutional autonomy.

Interoperability consequently depends upon several mutually reinforcing dimensions. Normative interoperability establishes sufficiently compatible conceptual foundations to support cooperation. Legal interoperability¹¹⁵ provides compatible rules governing authority, liability, recognition and remedies. Organizational interoperability aligns institutional mandates, governance arrangements and operational responsibilities. Semantic interoperability preserves the meaning, provenance and interpretability of information across institutional contexts. Technical interoperability supplies the protocols, interfaces, cybersecurity mechanisms and trust services through which authorized interactions become operational. Together, these dimensions show why interoperability is best understood as governed cooperation rather than mere connectivity.

These dimensions should not be understood as independent layers but as complementary components of a single governance architecture. Abbott and Snidal have shown that contemporary governance increasingly relies upon standards that coordinate behavior without replacing domestic legal authority.¹¹⁶ Digital interoperability reflects precisely this dynamic. Common standards enable institutions to cooperate while preserving legal autonomy, provided that such standards remain subject to legitimate governance and democratic accountability. Technical compatibility without legal authority may facilitate unlawful processing; legal compatibility without organizational coordination frequently remains

¹¹⁵ Rolf H Weber, *Legal Interoperability as a Tool for Combatting Fragmentation* (Global Commission on Internet Governance Paper Series No 4, Centre for International Governance Innovation, December 2014); Luca Belli and Danilo Doneda, 'Data Protection in the BRICS Countries: Legal Interoperability through Innovative Practices and Convergence' (2023) 13(1) *International Data Privacy Law* 1–24; Luca Belli and Nathalia Foditsch, 'Network Neutrality: An Empirical Approach to Legal Interoperability' in Luca Belli and Primavera De Filippi (eds), *Net Neutrality: Competing Perspectives on Freedom of Expression Online* (Springer 2016) 281–298

¹¹⁶ Kenneth W Abbott and Duncan Snidal, 'International "Standards" and International Governance' (2001) 8(3) *Journal of European Public Policy* 345–370; Kenneth W Abbott and Duncan Snidal, 'Strengthening International Regulation through Transnational New Governance: Overcoming the Orchestration Deficit' (2009) 42(2) *Vanderbilt Journal of Transnational Law* 501–578

ineffective; organizational cooperation without semantic coherence may generate incorrect administrative outcomes; and conceptual convergence without technical implementation remains merely aspirational. Data governance should therefore not be regarded as an additional dimension of interoperability, but as the normative framework that permeates each of these dimensions.

Interoperability should therefore be understood not as the antithesis of sovereignty but as one of its principal operational expressions. Properly governed interoperability enables cooperation without institutional uniformity, coordination without centralization and openness without loss of democratic control.¹¹⁷ It translates the integrated governance capacity described in Section III into the practical conditions of cooperation among sovereign equals developed in Section 4.1. Yet interoperability by itself remains a condition of legitimate interaction rather than a permanent institutional capability. For governed interoperability to become repeatable, trustworthy and scalable, it must be supported by shared infrastructures.

4.3. DIGITAL PUBLIC INFRASTRUCTURE AS SHARED FACILITATOR

The preceding section argued that interoperability is one of the principal operational expressions of sovereignty because it allows legally autonomous institutions to cooperate under shared rules without surrendering their mandates or decision-making authority. Digital Public Infrastructure occupies the next step in this argument. If interoperability describes the conditions under which systems and institutions can interact legitimately, DPI provides the shared capabilities that make such interaction repeatable, trustworthy and scalable.¹¹⁸ It is therefore not a parallel alternative to interoperability, but the infrastructural substrate through which governed interoperability becomes a durable expression of cooperative sovereignty.

Interoperability alone does not create cooperation; it merely enables the possibility of interaction. Durable cooperation requires institutional capabilities that can be reused across services, sectors and jurisdictions. DPI transforms interoperability from a set of technical, semantic, legal and organizational compatibilities into a persistent public capability. Once common trust services, credential frameworks, payment rails and data exchange mechanisms are established, new services need

¹¹⁷ Belli, L. and Bhinder, A. Cooperative Digital Sovereignty and Artificial Intelligence Promoting Resilience, Strategic Openness, and Self-Determination. (Digital Cooperation Organization, 2026).

¹¹⁸ Mila Samdub and Chand Rajendra-Nicolucci, 'What is Digital Public Infrastructure? Towards More Specificity' (*Tech Policy Press*, 25 November 2024); Mila T Samdub, '*Digital Public Infrastructure*' at *a Turning Point: From Definitions to Motivations* (Open Future, February 2025)

not recreate the institutional foundations of cooperation. Instead, trust becomes embedded in infrastructure through shared assurance levels, provenance rules, audit mechanisms, access controls and governance frameworks.

This institutional function is particularly significant in cross-border contexts. In a digital economy characterized by dependence on a limited number of proprietary infrastructures, shared DPI offers an alternative to both fragmentation and technological dependency. By relying on open standards, modular architectures and publicly governed trust frameworks, it enables cooperation without requiring reliance on a single platform or provider.¹¹⁹ This approach strengthens both institutional autonomy and competition by ensuring that foundational digital capabilities remain transparent, interoperable, contestable and accountable, while leaving ample space for innovation at the application layer.

Hence, DPI contributes to data sovereignty only when it remains modular, secure, auditable, interoperable and replaceable. Properly governed, it connects interoperability with a cooperative conception of digital sovereignty¹²⁰, enabling autonomous institutions to authenticate, exchange information and deliver digital services under shared governance arrangements while preserving legal diversity, democratic accountability and the sovereign equality of participating jurisdictions.

4.4. FROM DEPENDENCY TO RESILIENT INTERDEPENDENCE

The framework developed throughout this paper ultimately leads to a different understanding of data sovereignty as the institutional capacity to govern interdependence. The central challenge confronting contemporary states is therefore not whether digital ecosystems should be open or closed, but whether openness can be governed in ways that preserve democratic agency, institutional autonomy and constitutional accountability.

This distinction is fundamental because sovereignty has rarely implied complete self-sufficiency. Modern states have always relied upon trade, scientific exchange, financial systems, technical standards and international institutions. Their sovereignty has depended not upon eliminating interdependence, but upon participating in interdependent relationships under conditions of reciprocity, institutional autonomy and meaningful choice. The same principle applies to the digital economy.

¹¹⁹ Doctorow, C. (2021). *How to destroy surveillance capitalism*. Medium Editions.

¹²⁰ Belli, L. and Bhinder, A. Cooperative Digital Sovereignty and Artificial Intelligence Promoting Resilience, Strategic Openness, and Self-Determination. (Digital Cooperation Organization, 2026).

The relevant distinction is therefore not between openness and sovereignty, but between dependency and resilient interdependence. Dependency arises where reliance upon external infrastructures, technologies or governance arrangements substantially constrains the legitimate public choices of states and their institutions. A government may formally retain authority over its data, laws and public institutions while lacking the practical capacity to audit critical systems, substitute providers, preserve operational continuity, diversify technological options or ensure that the economic value generated through digital activities contributes to domestic development. Dependency is consequently not synonymous with reliance; it is reliance without meaningful institutional choice.

Resilient interdependence, by contrast, is fully compatible with sovereignty. It emerges when cooperation is structured through reciprocity, transparency, contestability, auditability, reversibility, diversification and institutional trust.¹²¹ Under these conditions, states remain connected without becoming captive, open without becoming subordinate and cooperative without relinquishing constitutional autonomy. A digital relationship should therefore be considered sovereign not because it is territorially enclosed, but because it preserves the capacity to revise technological choices, diversify infrastructures, enforce legal safeguards, audit systems, participate in value creation and contest governance arrangements over time.

The integrated governance framework developed in this paper explains how agency can be sustained. Constitutional and data governance establish the legal legitimacy and institutional allocation of authority. Digital Public Infrastructure provides the shared institutional capabilities through which governance becomes operational. Interoperability enables autonomous institutions and jurisdictions to cooperate through common standards and trusted governance arrangements while preserving their respective mandates. Cybersecurity safeguards the integrity and trustworthiness of shared infrastructures. Industrial and competition policies preserve technological capability, innovation and strategic choice, while fiscal capacity ensures that these arrangements remain financially and institutionally sustainable. Together, these dimensions constitute the institutional conditions through which sovereignty can be exercised within digitally interconnected societies.

¹²¹ Belli, L. and Bhinder, A. Cooperative Digital Sovereignty and Artificial Intelligence Promoting Resilience, Strategic Openness, and Self-Determination. (Digital Cooperation Organization, 2026); Belli L. and others, Soberania Digital e Inteligência Artificial no Brasil: Rumo à autonomia tecnológica (Lumen-Juris 2026).

The implications extend beyond data governance alone. Sovereignty in the digital ecosystem can no longer be evaluated exclusively through territorial jurisdiction, ownership of infrastructure or localisation of data. It must also be assessed according to whether states possess the institutional capacity to shape the technological, legal and economic conditions under which digital transformation unfolds.¹²² Data sovereignty should therefore not be understood as the capacity to prevent data from crossing borders, nor as the pursuit of technological autarky. It is the institutional capacity to determine the constitutional, legal, technological and economic conditions under which data, public authority and institutional trust may legitimately circulate across interconnected digital ecosystems.

CONCLUSIONS

This paper has argued that data sovereignty should not be understood as territorial control over data, nor as a synonym for data localization. Neither should it be reduced to the protection of personal information, however fundamental that objective remains. Rather, data sovereignty should be understood as the institutional capacity of individuals, societies and states to govern the generation, processing, exchange and use of data in accordance with democratically legitimate objectives. Importantly, this capacity does not arise from any single legal instrument or technological solution. It emerges from the interaction of multiple governance capacities that together enable societies to exercise meaningful agency within an increasingly interconnected digital economy.

The paper therefore proposed expanding the classical doctrine of informational self-determination. The historical evolution of that doctrine demonstrates its enduring importance. Beginning with the German Federal Constitutional Court's Census Decision and subsequently developing through European constitutional law, the jurisprudence of the Inter-American Court of Human Rights, Asian developmental strategies and African postcolonial scholarship, informational self-determination established an indispensable normative foundation for digital governance by protecting human dignity, personal autonomy and democratic participation. These values remain as essential today as they were four decades ago.

Yet the contemporary digital economy presents challenges that extend well beyond the relationship between individuals and those processing their personal information. Artificial intelligence systems rely upon unprecedented volumes of data. Cloud computing has transformed digital infrastructures into globally distributed ecosystems. Cyber operations increasingly target critical public services. A relatively small number of corporations exercise significant influence over cloud

¹²² Idem.

services, digital platforms, mobile operating systems and foundational AI models. At the same time, geopolitical competition has intensified around semiconductors, telecommunications infrastructure, software ecosystems and digital payment systems. Data have become not merely objects of legal protection but strategic resources whose governance increasingly shapes economic development, technological innovation and national resilience.

These transformations require a broader conceptual framework where informational self-determination remains necessary, but it is no longer sufficient. The paper therefore argued that data sovereignty should be understood as a multidimensional governance framework constituted by six mutually reinforcing capacities: the protection of fundamental rights through data protection; cybersecurity and digital resilience; technological governance through Digital Public Infrastructure; industrial development and technological capability; competition and innovation; and fiscal justice through equitable distribution of the value generated by data. Each of these dimensions addresses a distinct source of vulnerability within contemporary digital ecosystems. None, however, can independently produce sovereignty. Only their interaction creates the institutional conditions through which meaningful governance becomes possible.

The paper has also argued that data sovereignty possesses an essential international dimension. The digital economy is inherently transnational. Cloud computing, software development, artificial intelligence, digital trade and communication networks depend upon forms of cooperation that no country can realistically replace through complete technological self-sufficiency. The challenge confronting states is therefore not how to eliminate interdependence, but how to prevent interdependence from becoming structural dependency.

This distinction has acquired growing importance in recent years. The increasing fragmentation of the international system has demonstrated that technological and financial infrastructures may become instruments of geopolitical influence. Export controls on advanced semiconductors, restrictions affecting cloud services, limitations on access to digital technologies, and the strategic use of financial and technological infrastructures have illustrated that dependence upon external digital ecosystems may significantly constrain national policy choices.

In this context, the central conclusion of the paper is that data sovereignty should not be equated with digital isolationism. Attempts to isolate national digital ecosystems from international cooperation would not only prove economically costly but would also undermine many of the benefits generated by global scientific collaboration, digital trade and technological innovation. Equally, however, unrestricted dependence upon a limited number of foreign digital infrastructures risks creating structural asymmetries incompatible with meaningful sovereign equality.

The alternative proposed in this paper is one of cooperative sovereignty. Building data sovereignty requires cooperation grounded in shared concepts, interoperable technical standards, compatible legal frameworks, trusted cybersecurity architectures and common institutional principles. Sovereignty is therefore strengthened when states cooperate to develop open Digital Public Infrastructures, coordinate cybersecurity standards, establish trusted mechanisms for cross-border data governance and promote equitable participation in the digital economy.

The road ahead nevertheless remains challenging. Contemporary digital ecosystems remain characterised by significant concentration of technological capability, market power and infrastructural control. The enormous investments required for advanced semiconductors, hyperscale cloud computing, frontier artificial intelligence and global communication networks create barriers that few countries can overcome independently. The economic incentives favouring concentration remain powerful, while geopolitical competition continues to intensify. Under these conditions, the aspiration for data sovereignty should not be confused with the illusion of complete technological independence.

Instead, the objective should be to strengthen governance capacity progressively through institution-building. Investments in Digital Public Infrastructure, cybersecurity, digital skills, domestic innovation ecosystems, open standards and regional cooperation can gradually reduce structural dependencies while preserving the benefits of an open digital economy. Middle-income and developing countries, in particular, are unlikely to achieve meaningful digital sovereignty acting in isolation. Cooperation among countries facing similar developmental challenges therefore becomes not merely desirable but strategically necessary.

Ultimately, sovereignty has always evolved alongside transformations in the organization of political and economic power. The emergence of the territorial state redefined sovereignty during the early modern period. Industrialization transformed it once again by linking political authority to economic and technological capacity. Today, the digital revolution is generating a comparable transformation. In the twenty-first century, sovereignty is increasingly exercised through the governance of data, algorithms, digital infrastructures and the institutions that sustain them.

The central argument of this paper may therefore be stated simply. Building data sovereignty requires expanding informational self-determination beyond its traditional individualistic foundations to encompass cybersecurity, Digital Public Infrastructure, industrial development, competition, fiscal justice and international cooperation. Only through this multidimensional framework can digital transformation contribute not merely to economic growth, but to human dignity, democratic resilience and sustainable development.

Da Autodeterminação Informativa à Soberania dos Dados: Um Framework de Governança

Luca Belli, Ana Brian, Armando Manzueta, Nicolo Zingales

INTRODUÇÃO: DESVENDANDO A SOBERANIA DOS DADOS

Poucos conceitos ganharam tanta proeminência na governança digital na última década quanto a soberania de dados, soberania digital e soberania de IA.¹ De fato, governos e outros atores cada vez mais invocam preocupações relacionadas à soberania ao discutir computação em nuvem, inteligência artificial (IA), cibersegurança, fluxos de dados transfronteiriços, infraestrutura pública digital, tributação de plataformas digitais ou autonomia tecnológica estratégica. Organizações internacionais também abraçaram o conceito ao buscarem conciliar

¹ See for instance Couture, S., & Toupin, S. (2019). What does the notion of “sovereignty” mean when referring to the digital? *New Media & Society*, 21(10), 2305-2322 ; Floridi, L. (2020) The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. *Philos. Technol.* 33, 369–378; Belli L (2021) BRICS countries to build digital sovereignty. In: Belli, L. (Ed.). *CyberBRICS: Cybersecurity Regulations in the BRICS Countries*. Cham: Springer. pp 271–280; Belli, L. (2023). ; Kovacs, A., Ranganathan, N. (2019). *Data sovereignty, of whom? Limits and suitability of sovereignty frameworks for data in India*. Data Governance Network Working Paper 03; Luca Belli, 'Building Good Digital Sovereignty through Digital Public Infrastructures and Digital Commons in India and Brazil' (T20 India 2023); Luca Belli, 'To Get Its AI Foothold, Brazil Needs to Apply the Key AI Sovereignty Enablers (KASE)' in S Feldstein (ed), *New Digital Dilemmas: Resisting Autocrats, Navigating Geopolitics, Confronting Platforms* (Carnegie 2023); Chander, A., & Sun, H. (Eds.). (2023). *Data Sovereignty: From the Digital Silk Road to the Return of the State*. Oxford University Press; Belli, L., 'BRICS countries and AI sovereignty: Introduction to Thematic Section' (2024) 34 *AJIC* 1, 1–6; Belli, L. (2025). Exploring the Key AI Sovereignty Enablers (KASE) of Brazil, to Build an AI Sovereignty Stack. In: Belli, L. and Gaspar W.B. (eds), *The Quest for AI Sovereignty, Transparency and Accountability* (Springer-Nature 2025); Belli, Nicolo Zingales, Building sovereign and integrated data governance, from Latin America to the G20, *International Data Privacy Law*, Volume 15, Issue 4, November 2025, Pages 319–322; Belli L. and others, *Soberania Digital e Inteligência Artificial no Brasil: Rumo à autonomia tecnológica* (Lumen-Juris 2026); Belli, L. *Data Sovereignty Doesn't Mean Data Isolationism*. Tech Policy press (15 July 2026).

os benefícios de uma economia digital aberta com crescentes preocupações sobre segurança, privacidade, concentração econômica e rivalidade geopolítica.²

No entanto, apesar de seu uso crescente, a soberania dos dados continua sendo um conceito elusivo e contestado. Diferentes atores empregam o termo para avançar objetivos muito distintos. Para alguns, ela diz principalmente respeito à proteção da privacidade individual por meio de leis robustas de proteção de dados. Outros a entendem como garantia da autoridade estatal sobre os dados gerados dentro das fronteiras nacionais, frequentemente defendendo requisitos de localização ou restrições às transferências transfronteiriças.³ Outros ainda enquadram a soberania dos dados como uma questão de independência tecnológica, enfatizando infraestrutura doméstica de nuvem, produção de semicondutores, capacidades de inteligência artificial ou identidades digitais seguras.

Cada vez mais, economistas e organizações internacionais reconhecem os dados como um fator estratégico de produção⁴ que sustenta a inovação, inteligência artificial e mercados digitais. Esse reconhecimento crescente chamou atenção para a concentração de infraestruturas de dados e digitais, levantando preocupações sobre concorrência, poder de mercado e inovação. Ao mesmo tempo, estudiosos do desenvolvimento e organizações internacionais como a Conferência das Nações Unidas sobre Comércio e Desenvolvimento (UNCTAD) enfatizaram que o valor gerado pelos fluxos globais de dados permanece altamente concentrado, com países em desenvolvimento frequentemente contribuindo com dados enquanto capturam apenas uma parcela limitada dos benefícios econômicos resultantes.⁵

Essas diversas compreensões revelam que a soberania dos dados se tornou um conceito multidimensional situado na interseção do direito constitucional, direito internacional, cibersegurança, economia, políticas tecnológicas e estudos de desenvolvimento. No entanto, grande parte da literatura existente – e dos especialistas que a desenvolvem – continua a analisar essas dimensões separadamente, tratando privacidade, cibersegurança, política industrial ou infraestrutura digital como domínios políticos distintos. Essa fragmentação

² Belli, L. and Bhinder, A. Cooperative Digital Sovereignty and Artificial Intelligence Promoting Resilience, Strategic Openness, and Self-Determination. (Digital Cooperation Organization, 2026).

³ Brian Nougères, A. (2026). *International collection of personal data* (UN Doc. A/HRC/61/48). United Nations, Human Rights Council.

⁴ Mayer-Schönberger, V., & Cukier, K. (2013). *Big Data: A revolution that will transform how we live, work, and think*. Houghton Mifflin Harcourt.

⁵ UNCTAD. (2019) Digital Economy Report 2019: Value Creation and Capture—Implications for Developing Countries; UNCTAD. (2021). *Digital Economy Report 2021: Cross-border Data Flows and Development: For Whom the Data Flow*; World Bank. (2021). *World Development Report 2021: Data for Better Lives*. Washington DC: World Bank.

obscurece a transformação mais ampla que está ocorrendo atualmente na governança digital.

Este artigo argumenta que a soberania dos dados deve, em vez disso, ser entendida como uma estrutura integrada de governança. Com base na definição proposta em pesquisas anteriores, definimos soberania de dados como “a capacidade institucional de indivíduos, sociedades e Estados de entender como funcionam as tecnologias de processamento de dados, desenvolver alternativas e regulá-las de forma eficaz, alcançando assim autodeterminação informativa e redistribuição justa de valor, de acordo com objetivos democraticamente determinados.”⁶ Esses objetivos incluem a proteção dos direitos fundamentais, responsabilidade democrática, desenvolvimento econômico, inovação tecnológica e concorrência saudável, cibersegurança e justiça social.

Essa compreensão deliberadamente se afasta de interpretações que reduzem a soberania à localização de dados.⁷ A localização pode, em certas circunstâncias, contribuir para a soberania, especialmente quando se trata de segurança nacional ou fiscalização regulatória.⁸ No entanto, a localização sozinha não pode garantir controle significativo sobre os dados se o software, infraestrutura de nuvem, hardware, padrões e plataformas pelas quais os dados circulam permanecerem controlados externamente. Um país pode exigir que os dados permaneçam fisicamente dentro de seu território, enquanto continua dependendo quase inteiramente de sistemas operacionais estrangeiros, provedores de nuvem, infraestruturas de pagamento, modelos de inteligência artificial e tecnologias de cibersegurança. Por outro lado, um país pode participar ativamente dos fluxos de dados transfronteiriços, mantendo uma capacidade soberana substancial por meio de instituições interoperáveis, estruturas jurídicas robustas, capacidades tecnológicas domésticas e infraestruturas digitais diversificadas.

⁶Belli, L., Gaspar W.B. and Singh, S. (2024). Data sovereignty and data transfers as fundamental elements of digital transformation: Lessons from the BRICS countries. *Computer Law & Security Review*, vol. 54.

⁷ López González, J., Casalini, F., & Porras, J. (2022). *A Preliminary Mapping of Data Localisation Measures*. OECD Trade Policy Papers No. 262. OECD Publishing; Svantesson, D. (2020). *Data Localisation Trends and Challenges: Considerations for the Review of the Privacy Guidelines*. OECD Digital Economy Papers No. 301.

⁸ Yayboke, E., Ramos, C. G., & Sheppard, L. R. (2021). *The Real National Security Concerns over Data Localization*. Center for Strategic and International Studies (CSIS); López González, J., Casalini, F., & Porras, J. (2023). *The Nature, Evolution and Potential Implications of Data Localisation Measures*. OECD Trade Policy Papers No. 278. OECD Publishing; Greenleaf, G. (2023). *Personal Data Localisation and Sovereignty along Asia's New Silk Roads*. In A. Chander & H. Sun (Eds.), *Data Sovereignty: From the Digital Silk Road to the Return of the State*. Oxford University Press

Assim, este documento propõe uma concepção mais ampla de soberania centrada na capacidade de governança, em vez da exclusividade territorial. Ou seja, defendemos que o conceito de soberania, quando aplicado às tecnologias digitais, deve ser visto como a capacidade de indivíduos, sociedades e Estados de moldar as regras que regem os ecossistemas de dados e de exercer uma agência significativa sobre a transformação digital sem se tornar estruturalmente dependente de atores externos tecnológicos, econômicos ou políticos.⁹

APRIMORANDO A AUTODETERMINAÇÃO INFORMATIVA

As origens intelectuais desse argumento desenvolvidas neste artigo estão na doutrina da autodeterminação informativa. Desenvolvida pelo Tribunal Constitucional Federal Alemão em sua histórica Decisão do Censo de 1983 (Volkszählungsurteil), a autodeterminação informativa reconheceu que os indivíduos devem manter a capacidade de determinar a divulgação e o uso de suas informações pessoais para preservar a dignidade humana e a liberdade democrática.¹⁰ Esse princípio essencial¹¹ influenciou profundamente o direito europeu de proteção de dados e posteriormente foi incorporado na Carta dos Direitos Fundamentais da União Europeia e no Regulamento Geral de Proteção de Dados (GDPR). Desenvolvimentos constitucionais semelhantes surgiram posteriormente dentro do sistema interamericano de direitos humanos.¹²

Até hoje, a autodeterminação informativa continua sendo um pilar indispensável da proteção de dados. Privacidade, dignidade, autonomia e participação democrática continuam a constituir os fundamentos normativos da governança digital. No

⁹ Sobre isso, ver Luca Belli, 'To Get Its AI Foothold, Brazil Needs to Apply the Key AI Sovereignty Enablers (KASE)' in S Feldstein (ed), *New Digital Dilemmas: Resisting Autocrats, Navigating Geopolitics, Confronting Platforms* (Carnegie 2023); Belli, L. (2025). Exploring the Key AI Sovereignty Enablers (KASE) of Brazil, to Build an AI Sovereignty Stack. In: Luca Belli and Walter B Gaspar (eds), *The Quest for AI Sovereignty, Transparency and Accountability* (Springer-Nature 2025); Luca Belli, Nicolo Zingales, Building sovereign and integrated data governance, from Latin America to the G20, *International Data Privacy Law*, Volume 15, Issue 4, November 2025, Pages 319–322; Luca Belli and others, *Soberania Digital e Inteligência Artificial no Brasil: Rumo à autonomia tecnológica* (Lumen-Juris 2026).

¹⁰ Federal Constitutional Court of Germany (BVerfG), Judgment of 15 December 1983 (Volkszählungsurteil / Census Act Decision), Case Nos 1 BvR 209, 269, 362, 420, 440, 484/83, BVerfGE 65, 1.

¹¹ Brian Nougères, A. (2022). Principles underpinning privacy and the protection of personal data (UN Doc. A/77/196). United Nations, General Assembly.

¹² Principalmente, o caso CAJAR será discutido na seção 1.2. Inter-American Court of Human Rights, Case of the Members of the José Alvear Restrepo Lawyers' Collective (CAJAR) v Colombia (Preliminary Objections, Merits, Reparations, and Costs), Judgment of 18 March 2024, Series C No 522

entanto, a economia digital, as tendências geopolíticas e a dinâmica de dependência tecnológica do século XXI diferem fundamentalmente do ambiente tecnológico em que a doutrina foi originalmente concebida.

A Decisão do Censo Alemão abordou os riscos apresentados pelos bancos de dados governamentais centralizados durante uma era em que o processamento de informações continuava relativamente limitado, em grande parte nacional, e a informação ainda não havia se tornado um ativo comercializado.¹³ Os ecossistemas digitais contemporâneos, por outro lado, são caracterizados por computação em nuvem distribuída globalmente e altamente concentrada, ecossistemas de inteligência artificial (IA), sensores onipresentes, tomada de decisão algorítmica, economias de plataforma, fluxos de dados transfronteiriços e ameaças cibernéticas cada vez mais sofisticadas motivadas tanto por fins financeiros quanto políticos. Os dados evoluíram de registros administrativos para um dos principais fatores de produção dentro da economia global. Sua governança, portanto, levanta questões que vão muito além da privacidade individual.

Hoje, a incapacidade de proteger infraestruturas digitais pode comprometer a soberania nacional, independentemente da existência e força da legislação de privacidade. A dependência de provedores de nuvem estrangeiros pode limitar a autonomia do setor público, mesmo quando os dados pessoais permanecem legalmente protegidos. Mercados digitais concentrados podem reduzir a inovação doméstica, apesar das salvaguardas constitucionais robustas. Da mesma forma, a tributação desigual de modelos de negócios altamente digitalizados pode agravar a concentração de riqueza, ao mesmo tempo em que priva os governos dos recursos fiscais necessários para investir em infraestruturas digitais seguras e inclusivas.

Esses desenvolvimentos sugerem que a autodeterminação informativa deve ser expandida, e não substituída. Os valores fundamentais que sustentam a doutrina — dignidade humana, autonomia e responsabilidade democrática — permanecem plenamente relevantes. No entanto, agora elas devem ser interpretadas dentro de um arcabouço de governança mais amplo, capaz de lidar com a dependência tecnológica, a concentração econômica, os riscos de cibersegurança e as

¹³ In this latter perspective see Julie E Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford University Press 2019); Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Public Affairs 2019); Wayne Wei Wang, 'China's Digital Transformation: Data-Empowered State Capitalism and Social Governmentality' (2023) 31 *African Journal of Information and Communication* 1. In this latter perspective see Julie E Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford University Press 2019); Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Public Affairs 2019); Wang, W. W. 'China's Digital Transformation: Data-Empowered State Capitalism and Social Governmentality' (2023) 31 *African Journal of Information and Communication* 1.

desigualdades de desenvolvimento, sem focar exclusivamente na proteção dos direitos individuais, mas também nos interesses coletivos, como segurança nacional, desenvolvimento econômico, concorrência saudável, inovação e progresso científico.¹⁴

Assim, este artigo propõe uma concepção de soberania de dados que se baseia em seis dimensões mutuamente reforçadoras:

- autodeterminação informativa por meio de proteção robusta de dados e direitos fundamentais;
- cibersegurança e resiliência digital;
- soberania tecnológica e Infraestrutura Pública Digital;
- desenvolvimento industrial e capacidades tecnológicas;
- concorrência e inovação nos mercados digitais;
- justiça fiscal por meio da tributação e mecanismos que promovam a distribuição equitativa do valor gerado pelos dados.

Essas dimensões não devem ser entendidas como objetivos políticos separados. Na verdade, elas constituem componentes complementares de uma única arquitetura de governança. Portanto, assim como fortalecer uma dimensão pode ser bem-intencionado, mas não eficaz, a fraqueza em qualquer dimensão acaba minando a soberania como um todo.

SOBERANIA DOS DADOS COMO CAPACIDADE DE GOVERNANÇA

Essa abordagem multidimensional também desafia as compreensões tradicionais da própria soberania. O direito internacional clássico concebia a soberania principalmente em termos territoriais.¹⁵ Os Estados exerciam autoridade suprema dentro de fronteiras geográficas claramente definidas, enquanto o direito

¹⁴ Sobre esta última perspectiva, ver Julie E Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford University Press 2019); Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Public Affairs 2019); Wayne Wei Wang, 'China's Digital Transformation: Data-Empowered State Capitalism and Social Governmentality' (2023) 31 *African Journal of Information and Communication* 1. In this latter perspective see Julie E Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford University Press 2019); Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Public Affairs 2019); Wang, W. W. 'China's Digital Transformation: Data-Empowered State Capitalism and Social Governmentality' (2023) 31 *African Journal of Information and Communication* 1.

¹⁵ Besson S. Sovereignty. in Peters A. & Wolfrum R. *Max Planck Encyclopedias of International Law*. Oxford University Press. (2021).

internacional regulava as relações entre entidades soberanas formalmente iguais. Embora a jurisdição territorial continue essencial, as tecnologias digitais operam cada vez mais por meio de infraestruturas transnacionais que desconsideram as fronteiras convencionais. Infraestrutura crítica de informação, como computação em nuvem, cabos submarinos, plataformas globais, modelos de IA e sistemas internacionais de pagamento digital funcionam em múltiplas jurisdições simultaneamente.

Como consequência, a soberania não pode mais ser compreendida exclusivamente por meio do controle territorial. A governança eficaz depende cada vez mais da capacidade industrial e institucional, da competência e escolha tecnológica, e da cooperação internacional. Estados capazes de maximizar opções – incluindo desenvolver – identidades digitais seguras, sistemas de pagamento interoperáveis, plataformas confiáveis de troca de dados e arquiteturas resilientes de cibersegurança podem exercer soberania consideravelmente maior do que Estados que dependem inteiramente de infraestruturas desenvolvidas externamente, independentemente de onde os dados estejam fisicamente armazenados.

Essa mudança do controle territorial para a capacidade de governança tem importantes implicações normativas. Sugere que a soberania não deve ser medida pelo volume de dados retidos dentro das fronteiras nacionais, mas pela capacidade de estabelecer estruturas legítimas e eficazes que regem seu ciclo de vida. Tais estruturas abrangem proteções legais, padrões tecnológicos, arranjos institucionais, estruturas de mercado e políticas fiscais. A soberania dos dados, portanto, torna-se uma capacidade institucional e regulatória dinâmica, em vez de um atributo territorial estático.

Importante, essa concepção evita a falsa dicotomia entre abertura e soberania. A participação nos fluxos globais de dados não precisa diminuir a soberania, desde que tal participação ocorra sob condições de escolha significativa, cooperação recíproca e resiliência institucional. Por outro lado, o isolamento dos ecossistemas digitais internacionais não aumenta automaticamente a soberania se a dependência tecnológica apenas se desloca de um ator externo para outro.¹⁶

ESTRUTURA DO ARTIGO

O restante deste artigo desenvolve esse argumento em quatro seções. A Seção I examina a evolução histórica da autodeterminação informativa em diferentes tradições jurídicas e políticas. Começando com a Decisão do Censo Alemão, traça a subsequente incorporação da autodeterminação informativa ao direito constitucional europeu, o sistema interamericano de direitos humanos, as abordagens de desenvolvimento asiáticas e as críticas pós-coloniais africanas à

¹⁶ Chander, A., & Lê, U. P. (2015). Data nationalism. *Emory Law Journal*, 64(3), 677-739.

dependência digital. A seção demonstra que, embora essas tradições diferam significativamente, compartilham uma preocupação comum em preservar a autonomia humana e coletiva sob condições de expansão do poder digital.

A Seção II argumenta que a transformação digital contemporânea exige a expansão da autodeterminação informativa para uma concepção mais ampla de soberania de dados. Examina como ameaças cibernéticas, evoluções da IA, dinâmicas de computação em nuvem, concentração de plataformas e infraestruturas digitais alteram fundamentalmente as condições sob as quais a autonomia informativa pode ser exercida.

A Seção III desenvolve o arcabouço analítico central do artigo ao examinar as seis dimensões interdependentes da soberania de dados: proteção de dados, cibersegurança, Infraestrutura Pública Digital, política industrial, concorrência e inovação, e justiça fiscal. É dada ênfase especial à Infraestrutura Pública Digital como a arquitetura tecnológica pela qual a governança soberana pode ser operacionalizada.

Por fim, a Seção IV explora como a soberania pode ser construída por meio da cooperação internacional, em vez do isolamento digital. Baseando-se no princípio da igualdade soberana contido no Artigo 2 da Carta das Nações Unidas, argumenta que padrões interoperáveis, estruturas de governança compartilhada e arquiteturas institucionais colaborativas oferecem o caminho mais promissor para ecossistemas digitais resilientes e inclusivos.

O artigo conclui argumentando que, embora as infraestruturas digitais contemporâneas permaneçam altamente concentradas e a competição geopolítica continue a se intensificar, a soberania dos dados não deve ser entendida como uma aspiração à autarquia tecnológica.¹⁷ Em vez disso, representa a capacidade coletiva de Estados, sociedades e indivíduos de cooperar como iguais na formação do futuro da economia digital global.

METODOLOGIA

Este artigo adota uma metodologia jurídica e de políticas interdisciplinar que combina análise doutrinária do direito com análise institucional comparativa e pesquisa de políticas públicas. Ele se baseia em fontes jurídicas primárias, incluindo disposições constitucionais, legislação, decisões judiciais, instrumentos internacionais e documentos de política, bem como literatura acadêmica de direito, economia, ciência política, administração pública, cibersegurança e governança digital. O objetivo não é fornecer um levantamento exaustivo de cada disciplina, mas desenvolver uma estrutura analítica integrada capaz de explicar a soberania dos

¹⁷ Belli, L. Data Sovereignty Doesn't Mean Data Isolationism. Tech Policy press (15 July 2026).

dados como um conceito multidimensional que abrange dimensões jurídica, tecnológica, econômica, do desenvolvimento, cibersegurança e fiscal.

O artigo também se baseia em análises comparativas para identificar convergências e divergências entre diferentes tradições regulatórias, com atenção especial às abordagens europeias, americanas, asiáticas e africanas para autodeterminação informativa e governança de dados. Além disso, examina iniciativas internacionais contemporâneas relacionadas à Infraestrutura Pública Digital (DPI), governança de dados e cooperação digital, a fim de identificar princípios emergentes de interoperabilidade e soberania cooperativa.

A Inteligência Artificial Generativa foi empregada como ferramenta de apoio à pesquisa durante a preparação deste manuscrito. Especificamente, foi usada para auxiliar na síntese das pesquisas anteriores dos autores, melhorar a estrutura e a coerência do manuscrito, identificar literatura potencialmente relevante para verificação subsequente, refinar a linguagem e o estilo, e facilitar a organização das referências

1. DA AUTODETERMINAÇÃO INFORMATIVA À SOBERANIA DOS DADOS

O debate contemporâneo sobre soberania de dados encontra suas raízes normativas em uma das decisões constitucionais mais influentes do século XX: o julgamento do Tribunal Constitucional Federal Alemão de 15 de dezembro de 1983 sobre a Lei Federal do Censo (*Volkszählungsurteil*).¹⁸ Embora decidido em resposta a um censo administrativo aparentemente comum, o caso transformou fundamentalmente as compreensões constitucionais de privacidade, autonomia pessoal e poder estatal no que já começava a ser definido como "sociedade da informação".¹⁹

A controvérsia surgiu após a República Federal da Alemanha promulgar uma legislação autorizando a coleta de informações pessoais extensas por meio do censo nacional. Vários cidadãos contestaram a legislação, argumentando que o acúmulo e a possível combinação de informações pessoais pelas autoridades públicas criavam riscos que iam muito além dos propósitos imediatos da administração estatística. O

¹⁸ Federal Constitutional Court of Germany (BVerfG), Judgment of 15 December 1983 (*Volkszählungsurteil / Census Act Decision*), Case Nos 1 BvR 209, 269, 362, 420, 440, 484/83, BVerfGE 65, 1.

¹⁹ Veja, por exemplo, o trabalho seminal de Nora D. & Minc A. *L'informatisation de la société. Rapport à M. le Président de la République*. La Documentation française. 1978

raciocínio da Corte refletia não apenas preocupações com mudanças tecnológicas, mas também as lições constitucionais derivadas da experiência histórica da Alemanha com vigilância autoritária tanto durante o regime nacional-socialista quanto na República Democrática Alemã. Portanto, a decisão reconheceu que a liberdade democrática depende de limitar as assimetrias informacionais entre indivíduos e o Estado.

A Corte articulou um princípio constitucional que ficaria conhecido como direito à autodeterminação informativa (*informationelle Selbstbestimmung*). Derivando esse direito das garantias da dignidade humana e do livre desenvolvimento da personalidade contidas nos Artigos 1 e 2 da Lei Fundamental, a Corte decidiu que os indivíduos devem manter a autoridade para determinar, em princípio, a divulgação e o uso de suas informações pessoais. Derivando esse direito das garantias da dignidade humana e do livre desenvolvimento da personalidade contidas nos Artigos 1 e 2 da Lei Fundamental Alemã, o Tribunal decidiu que os indivíduos devem manter a autoridade para determinar, em princípio, a divulgação e o uso de suas informações pessoais. Sem tal autoridade, os cidadãos não conseguiriam antecipar como as informações sobre eles poderiam ser combinadas, interpretadas ou usadas no futuro. Essa incerteza, argumentou a Corte, inevitavelmente desencorajaria indivíduos a exercer uma ampla gama de liberdades fundamentais, participar da vida democrática ou expressar opiniões divergentes.

Importante, a relevância da Decisão do Censo foi muito além do reconhecimento de um novo direito à privacidade. Representou uma profunda reconceitualização da liberdade constitucional sob condições de processamento de informações. Em vez de ver a privacidade apenas como "o direito de ser deixado em paz"²⁰ que sustenta uma legítima reivindicação de proteção e confidencialidade da vida privada, a Corte entendeu a dimensão informativa da autonomia como exigindo controle significativo sobre a circulação e o uso de informações pessoais. Nessa perspectiva, a liberdade na sociedade da informação dependia não apenas de impedir a divulgação, mas de preservar a capacidade do indivíduo de tomar decisões informadas sobre a governança dos dados pessoais.

Essa percepção provou ser notavelmente presciente. Muito antes do surgimento da internet, computação em nuvem, análise de Big Data ou IA, a Corte previu que a agregação de informações aparentemente inocentes poderia alterar fundamentalmente a relação entre cidadãos e autoridade pública.²¹ O poder

²⁰ Warren S. & Brandeis L. The Right to Privacy. Harvard Law Review, Vol. 4, No. 5 (Dec. 15, 1890), pp. 193-220

²¹ Benkler, Y. (2006). *The wealth of networks: How social production transforms markets and freedom*. Yale University Press.

informativo, e não apenas a coerção física, tornou-se reconhecido como uma dimensão central da governança constitucional.

A doutrina da autodeterminação informativa exerceu posteriormente profunda influência sobre o direito europeu de proteção de dados, moldando desenvolvimentos legislativos em todo o continente e fornecendo a base filosófica sobre a qual os direitos digitais contemporâneos seriam posteriormente construídos.²² Ao mesmo tempo, sua ênfase na autonomia individual refletia as realidades tecnológicas e políticas do início dos anos 1980. A principal preocupação era a relação entre o cidadão e o Estado. Os mercados de dados pessoais ainda estavam em sua infância, plataformas digitais globais ainda não existiam e a cibersegurança ainda não havia se tornado uma preocupação central de políticas.

Como seções posteriores deste estudo argumentarão, essas transformações não exigem nem abandonar nem substituir a autodeterminação informativa, que adquire um papel ainda mais relevante. No entanto, os recentes desafios tecnológicos, assim como a dimensão geopolítica adquirida pelas dependências tecnológicas, exigem a expansão dessa concepção inicial de autodeterminação informativa para uma concepção mais rica e abrangente de soberania dos dados.

1.1. AUTODETERMINAÇÃO INFORMATIVA DO PRINCÍPIO CONSTITUCIONAL AO MODELO REGULATÓRIO

A doutrina da autodeterminação informativa articulada pelo Tribunal Constitucional Federal Alemão rapidamente transcendeu suas origens nacionais para se tornar um dos princípios definidores da governança digital europeia.²³ Embora o conceito em si permanecesse enraizado na jurisprudência constitucional alemã, seus valores subjacentes de dignidade humana, autonomia e participação democrática orientaram progressivamente o desenvolvimento do direito da União Europeia, transformando a proteção de dados de uma preocupação administrativa em um compromisso constitucional.

Essa evolução refletiu o projeto constitucional europeu mais amplo. Após a Segunda Guerra Mundial, a integração europeia foi construída sobre a convicção de que a cooperação econômica deveria ser acompanhada pela proteção dos direitos fundamentais e do Estado de Direito. À medida que as tecnologias digitais se

²² Streinz T. "The Evolution of European Data Law" in Craig P. and de Búrca G. (eds), *The Evolution of EU Law* (Oxford University Press, 3rd edn 2021) chapter 29.

²³ Brian Nougères, A. (2022). *Principles underpinning privacy and the protection of personal data* (UN Doc. A/77/196). United Nations, General Assembly.

expandiram nas últimas décadas do século XX, as instituições europeias reconheciam cada vez mais que a proteção das informações pessoais constituía uma condição prévia essencial para o efetivo desfrute da liberdade individual dentro de um mercado interno integrado.²⁴

A adoção da Diretiva 95/46/CE representou um passo decisivo nessa direção. Embora tenha como principal objetivo harmonizar a legislação nacional para facilitar a livre circulação de dados pessoais dentro da União Europeia, a Diretiva também refletia uma ambição constitucional mais profunda. Os dados pessoais não eram mais tratados apenas como informações comerciais, mas como uma extensão da personalidade individual, merecendo proteção legal independentemente de considerações econômicas. A Diretiva, portanto, estabeleceu princípios comuns que regem a coleta, o processamento e a transferência de dados pessoais, ao mesmo tempo em que facilitava o funcionamento do mercado interno.

A constitucionalização da proteção de dados atingiu um novo estágio com a Carta dos Direitos Fundamentais da União Europeia.²⁵ Significativamente, a Carta distinguiu entre o respeito à vida privada, protegido pelo Artigo 7, e a proteção dos dados pessoais sob o Artigo 8. Essa distinção foi sem precedentes no direito constitucional comparado. Em vez de considerar a proteção de dados apenas como um aspecto da privacidade, a União Europeia a reconheceu como um direito fundamental autônomo com seu próprio conteúdo normativo. O artigo 8 estabeleceu ainda que os dados pessoais devem ser tratados de forma justa, para fins específicos e com base em consentimento ou outro fundamento legal legítimo, garantindo direitos de acesso e retificação sob supervisão de autoridades independentes.

Essa arquitetura constitucional encontrou posteriormente sua expressão mais abrangente no Regulamento Geral de Proteção de Dados (GDPR). Entrando em vigor em 2018, o GDPR buscou não apenas harmonizar a legislação europeia de proteção de dados, mas também responder ao surgimento de plataformas digitais globais, processamento algorítmico em larga escala e fluxos de dados transfronteiriços cada vez mais complexos. O Regulamento ampliou significativamente a gama de direitos individuais por meio de mecanismos como portabilidade de dados, direito de "ser esquecido" ou direito de apagamento, aumento das obrigações de responsabilização, privacidade desde o design e por padrão, e restrições à tomada

²⁴ Erdos D. "The Development of European Data Protection Law and Regulation" in Erdos D. *European Data Protection Regulation, Journalism, and Traditional Publishers*. (Oxford University Press, 2019).

²⁵ Ibid and supra n (17).

de decisão automatizada. Ao mesmo tempo, fortaleceu as autoridades de supervisão e introduziu sanções administrativas substanciais.

A importância global do GDPR vai muito além da Europa. Por meio de sua aplicação extraterritorial, mecanismos de adequação e influência sobre a legislação nacional em múltiplas jurisdições, o Regulamento contribuiu para o que estudiosos frequentemente descrevem como o "Efeito Bruxelas"²⁶: a capacidade da regulação europeia de moldar a governança global dos dados por meio do poder de mercado e do lobby regulatório, em vez da coerção territorial.²⁷ Países da América Latina, África e Ásia têm alinhado cada vez mais a legislação doméstica aos princípios do GDPR para facilitar o comércio internacional e as transferências de dados, tornando os padrões europeus de proteção de dados um ponto de referência importante na convergência regulatória global.²⁸

No entanto, apesar de suas conquistas notáveis, o modelo europeu permanece fundamentalmente centrado na relação entre indivíduos e aqueles que processam seus dados pessoais. Seu principal objetivo é proteger a autonomia individual contra o processamento de dados ilegal ou desproporcional. O grau em que o atual quadro de proteção de dados consegue alcançar tal objetivo de forma eficaz, em vez de apenas fornecer uma fachada de conformidade, é objeto de intensos debates e pode levar a questionar a capacidade da lei de proteção de dados de garantir concretamente os direitos individuais.²⁹

Além disso, embora o GDPR contenha disposições importantes relacionadas à segurança, responsabilidade e transferências internacionais, ele não aborda diretamente questões mais amplas sobre dependência tecnológica, capacidade industrial, concentração de mercado ou assimetrias geopolíticas dentro da economia digital. Essas questões ficam cada vez mais fora dos limites conceituais da autodeterminação informativa como tradicionalmente entendidos.

Iniciativas europeias recentes – incluindo a Lei de Governança de Dados, a Lei de Dados, a Lei dos Mercados Digitais, a Lei dos Serviços Digitais, a Lei de Inteligência Artificial, o marco de Soberania da Nuvem e a estratégia europeia para a Infraestrutura Pública Digital – sugerem que a própria União Europeia começou a ir

²⁶ Bradford, A. 'The Brussels Effect' (2012) 107 Nw U L Rev 1, 3, 6.

²⁷ Bradford, A. 'The Brussels Effect' (2012) 107 Nw U L Rev 1, 3, 6.

²⁸ Brian Nougères, A. (2022). *Privacy and personal data protection in Ibero-America: A step towards globalization?* (UN Doc. A/HRC/49/55). United Nations, Human Rights Council; Carrillo A.J. and Jackson, M. Follow the Leader? A Comparative Law Study of the EU's General Data Protection Regulation's Impact in Latin America. ICL Journal 2022; 16(2): 177–262.

²⁹ Li W. and others. Mapping the empirical literature of the GDPR's (In-)effectiveness: A systematic review. Computer Law & Security Review. 57 (2025) 106129

além de uma abordagem puramente centrada na privacidade. Coletivamente, esses instrumentos buscam regular os dados não apenas como objeto de direitos individuais, mas como recurso econômico, ativo estratégico e componente da infraestrutura crítica.³⁰ Ao fazer isso, a governança digital europeia reflete cada vez mais uma concepção mais ampla de soberania, mesmo que essa evolução ainda não tenha sido totalmente articulada em termos conceituais.

1.2. AUTODETERMINAÇÃO INFORMATIVA NO SISTEMA INTERAMERICANO DE DIREITOS HUMANOS

Desenvolvimentos dentro do sistema interamericano de direitos humanos revelam uma evolução paralela, porém distinta, da autodeterminação informativa. Embora as tradições constitucionais latino-americanas historicamente tenham dado grande ênfase à privacidade e aos "dados de *habeas corpus*",³¹ o surgimento das tecnologias digitais tem expandido progressivamente a compreensão da proteção de dados pessoais no âmbito dos direitos humanos.

Um marco particularmente significativo é a jurisprudência da Corte Interamericana de Direitos Humanos, que tem reconhecido cada vez mais que a coleta, o processamento e a disseminação de informações pessoais afetam diretamente o exercício das liberdades fundamentais garantidas pela Convenção Americana de Direitos Humanos. Em vez de enxergar os dados pessoais apenas como objetos de regulamentação administrativa, a Corte vinculou a autonomia informativa ao gozo efetivo da dignidade, liberdade de expressão, liberdade de associação e participação democrática.

Essa evolução encontra expressão importante no julgamento CAJAR, no qual a Corte reconheceu que a proteção das informações pessoais faz parte da garantia mais ampla da vida privada prevista no Artigo 11 da Convenção Americana. Essa evolução encontra expressão importante no julgamento CAJAR³², no qual a Corte reconheceu que a proteção das informações pessoais faz parte da garantia mais ampla da vida privada prevista no Artigo 11 da Convenção Americana. A decisão é particularmente notável porque situa a autodeterminação informativa dentro do quadro constitucional mais amplo da sociedade democrática. Vigilância, coleta ilegal de

³⁰ Plantin, J. C., Lagoze, C., Edwards, P. N., & Sandvig, C. (2018). Infrastructure studies meet platform studies in the age of Google and Facebook. *New Media & Society*, 20(1), 293-310

³¹ Alvim Wambier T.A. (Ed.), *Habeas Data*. São Paulo: RT, 1998; Guadamuz, A. *Habeas Data: The Latin-American Response to Data Protection*. *The Journal of Information Law and Technology*. v. 2, 2000.

³² Em especial, o caso CAJAR será discutido na seção 1.2. Inter-American Court of Human Rights, *Case of the Members of the José Alvear Restrepo Lawyers' Collective (CAJAR) v Colombia* (Preliminary Objections, Merits, Reparations, and Costs), Judgment of 18 March 2024, Series C No 522

informações pessoais e práticas arbitrárias de processamento não interferem apenas na privacidade; eles também podem minar a participação cívica, desencorajar o engajamento político e enfraquecer instituições democráticas.

A abordagem interamericana, portanto, complementa o modelo europeu ao mesmo tempo em que introduz uma ênfase particular na responsabilização democrática e na proteção de defensores dos direitos humanos, jornalistas e atores da sociedade civil. Em sociedades marcadas por uma história recente de autoritarismo, violência política e desigualdade estrutural, a autodeterminação informativa assume um papel particularmente importante na salvaguarda da participação democrática contra abusos de poder tanto públicos quanto privados.

A prática constitucional latino-americana também demonstra uma importante abertura para reconhecer direitos digitais como extensões de garantias constitucionais mais amplas. Várias constituições protegem explicitamente os dados de habeas corpus, concedendo aos indivíduos o direito de acessar, corrigir e atualizar informações sobre si mesmos mantidas em bancos de dados públicos ou privados.³³ Embora esses mecanismos difiram institucionalmente das autoridades europeias de proteção de dados, eles buscam objetivos semelhantes ao reforçar a agência individual sobre informações pessoais.

Ao mesmo tempo, porém, muitos países latino-americanos enfrentam desafios que vão além dos limites tradicionais da lei de privacidade. Juntamente com baixa maturidade institucional e alfabetização (especialmente em proteção de dados e funcionamento de tecnologias), capacidade tecnológica doméstica limitada, dependência de provedores estrangeiros de nuvem, concentração dos mercados digitais e participação desigual na economia global de dados levantam questões de que a autodeterminação informativa está longe de ser adequadamente abordada. Consequentemente, os debates sobre políticas digitais têm conectado cada vez mais a proteção de dados pessoais à política industrial digital, cibersegurança, inclusão digital e cooperação tecnológica.³⁴

Nesse sentido, a experiência interamericana ilustra uma tendência global mais ampla. A proteção de informações pessoais foi elevada ao status de objetivo constitucional essencial, mas tornou-se evidente que uma governança sustentável

³³ Carrillo A.J. and Jackson, M. Follow the Leader? A Comparative Law Study of the EU's General Data Protection Regulation's Impact in Latin America. *ICL Journal* 2022; 16(2): 177–262.

³⁴ Belli, L. & Bhinder. Cooperative Digital Sovereignty and Artificial Intelligence Promoting Resilience, Strategic Openness, and Self-Determination. Digital Cooperation Organization (2026); Belli L. Soberania Digital no Brasil Diagnóstico, Desafios e Caminhos sob a perspectiva da Ciência, Tecnologia e Inovação. Centro de Gestão e Estudos Estratégicos (CGEE). MCTI (Ministério da Ciência, Tecnologia e Inovação Brasília. (2026).

da transformação digital exige cada vez mais integrar direitos humanos com questões de desenvolvimento econômico, cibersegurança, capacidade tecnológica e resiliência institucional.

CONSIDERANDO AS PERSPECTIVAS ASIÁTICAS: UMA ABORDAGEM COLETIVA PARA A AUTODETERMINAÇÃO INFORMATIVA PARA SEGURANÇA E DESENVOLVIMENTO

Ao contrário das concepções europeia e interamericana, onde a autodeterminação informativa se desenvolveu principalmente como um direito constitucional individual que limita o exercício do poder estatal, muitas abordagens asiáticas para a governança de dados evoluíram dentro de uma concepção mais ampla da relação entre indivíduo, sociedade e Estado, com um foco muito mais pronunciado nos interesses coletivos. De fato, embora exista considerável diversidade na região, a governança digital frequentemente foi enquadrada não apenas em termos de proteção dos direitos individuais, mas também de promoção da estabilidade social, segurança nacional, modernização econômica e desenvolvimento tecnológico.³⁵

Essa divergência reflete tradições constitucionais distintas e trajetórias de desenvolvimento. Muitas economias asiáticas experimentaram rápida industrialização sob estados em desenvolvimento que coordenaram ativamente a modernização tecnológica, políticas industriais e investimentos em infraestrutura. Consequentemente, as tecnologias digitais muitas vezes foram vistas como ativos estratégicos que contribuem para o desenvolvimento nacional, em vez de apenas como domínios que exigem proteção legal contra interferência governamental.

Países como Singapura, República da Coreia, Japão, China e, mais recentemente, Índia ilustram diferentes manifestações dessa abordagem. A estratégia de governança digital de Singapura, por exemplo, combina proteção de dados pessoais com forte ênfase em infraestrutura digital confiável, cibersegurança e ecossistemas de inovação.³⁶ A Lei de Proteção de Dados Pessoais coexiste com iniciativas

³⁵ Greenleaf, G. (2014). Asian data privacy laws: Trade and human rights perspectives. Oxford University Press; Bo Zhao a , Yang Feng Mapping the development of China's data protection law: Major actors, core values, and shifting power relations. *Computer Law & Security Review* 40 (2021) 105498; Wang, W. 'China's Digital Transformation: Data-Empowered State Capitalism and Social Governmentality' (2023) 31 *African Journal of Information and Communication* 1; Belli L. & Chang S. Governança de dados na China: soberania, cibersegurança e proteção de dados rumo ao "Efeito Pequim". *Revista Brasileira de Direitos Fundamentais & Justiça*. v. 23 n. 52 (2025).

³⁶ Arif Perdana and Intan Azura Mokhtar, 'Digital Transformation in Government: Lessons from GovTech Singapore' (2025) *Journal of Information Technology Teaching Cases* 1 ; Wanning Sun, 'Artificial

nacionais abrangentes que promovem identidade digital, serviços públicos interoperáveis e transações digitais seguras, refletindo uma compreensão integrada da governança digital.

Da mesma forma, a República da Coreia historicamente vinculou a transformação digital à competitividade industrial.³⁷ O investimento governamental em infraestrutura de banda larga, fabricação de semicondutores, inteligência artificial e cibersegurança tem sido acompanhado por marcos regulatórios que buscam equilibrar a proteção da privacidade com a inovação. Aqui, a autodeterminação informativa opera junto com um compromisso explícito com a capacidade tecnológica e a resiliência econômica.

O Japão adotou uma abordagem comparável por meio de sua visão de "Fluxo Livre de Dados com Confiança" (DFFT), promovida durante sua presidência do G20 em 2019, e posteriormente endossada e incentivada pela OCDE³⁸. Em vez de defender fluxos de dados irrestritos ou exigências rigorosas de localização, a DFFT busca conciliar abertura com confiança combinando interoperabilidade internacional, proteção de privacidade, cibersegurança e padrões comuns de governança. Essa iniciativa ilustra uma importante mudança conceitual: a soberania não é alcançada por meio do isolamento, mas sim pela participação em ecossistemas digitais confiáveis regidos por regras compartilhadas.³⁹

Na China, a governança digital desenvolveu-se dentro de um arcabouço constitucional com maior ênfase nos interesses coletivos, na segurança nacional e no desenvolvimento liderado pelo Estado.⁴⁰ Legislações como a Lei de

Intelligence: Governing Singapore's Smart Digital Journey' (2024) 10(3) *Communication Research and Practice*

³⁷ Keun Lee, *The Art of Economic Catch-up: Barriers, Detours and Leapfrogging in Innovation Systems* (Cambridge University Press 2019); Keun Lee, 'How Can Korea Be a Role Model for Catch-up Development? A "Capability-based" View' (2019) 47(2) *Oxford Development Studies* 164–17.

³⁸ O conceito DFFT prescreve que garantir a confiança em termos de privacidade, segurança e direitos de propriedade intelectual é pré-requisito para o livre fluxo de dados através das fronteiras. Veja G20. "G20 Leaders' Declaration in Osaka". (June 29, 2019). Durante a presidência japonesa de 2023, também a Cúpula do G7 em Hiroshima endossou a "Visão dos Ministros da Tecnologia e Digital do G7 para operacionalizar o livre fluxo de dados com confiança e suas prioridades", incluindo o estabelecimento de um "Acordo de Parceria Institucional." Veja G7. Ministerial Declaration - The Meeting of the G7 Digital and Technology Ministers. (04/30/2023). Nesse contexto, a Declaração do G7 dos Ministros da Tecnologia e Digital afirmou ainda que "os atributos da OCDE e seu trabalho atual nas áreas de governança de dados, privacidade, livre fluxo de dados com confiança e economia digital tornam-na adequada para avançar esse esforço internacional" Veja G7.

Annex 1 of the digital and technology track – G7 vision to operationalize the DFFT and its priorities. (04/30/2023).

³⁹ Chander, A., & Lê, U. P. (2015). Data nationalism. *Emory Law Journal*, 64(3), 677-739.

⁴⁰

Cibersegurança, a Lei de Segurança de Dados e a Lei de Proteção de Informações Pessoais demonstram que a China reconhece a privacidade e a proteção das informações pessoais como valores legais importantes. No entanto, esses objetivos são explicitamente integrados a metas mais amplas relacionadas à segurança nacional, competitividade industrial e soberania tecnológica.

Embora os arranjos institucionais difiram substancialmente das tradições constitucionais liberais, a experiência chinesa ressalta um ponto importante para a presente análise: a governança de dados se estende cada vez mais além da privacidade individual, abrangendo capacidade tecnológica, cibersegurança e desenvolvimento econômico.⁴¹ Seja por meio de instituições democráticas liberais ou de modelos de governança mais centralizados, os Estados contemporâneos reconhecem cada vez mais que os dados constituem infraestrutura estratégica que exige governança pública coordenada.

Talvez o desenvolvimento recente mais significativo tenha surgido na Índia com a construção do que ficou conhecido como India Stack.⁴² Combinando identidade digital (Aadhaar), pagamentos digitais (UPI), autenticação de documentos, compartilhamento de dados baseado em consentimento e outras infraestruturas públicas digitais interoperáveis, a Índia demonstrou que os governos podem criar arquiteturas digitais fundamentais que promovam simultaneamente inclusão, inovação e prestação de serviços públicos. Embora os debates sobre privacidade, vigilância e exclusão continuem importantes, a experiência indiana alterou fundamentalmente as discussões internacionais sobre a relação entre infraestrutura tecnológica, governança de dados e soberania.⁴³

O conceito de Infraestrutura Pública Digital (DPI), agora cada vez mais promovido pelo G20, pelo Programa das Nações Unidas para o Desenvolvimento e por diversas instituições de desenvolvimento, deve muito a essa experiência. Em vez de depender exclusivamente da regulamentação para moldar os mercados digitais, o DPI busca incorporar valores normativos diretamente na arquitetura tecnológica. Sistemas de identidade digital, infraestruturas de pagamento e mecanismos confiáveis de troca de dados tornam-se infraestruturas institucionais que apoiam tanto os direitos individuais quanto o desenvolvimento econômico.

Wang. W.W. Chang S. Chen S. Assessing the Chinese Personal Information Protection Law (PIPL) e Beyond: The Stakeholder Architecture of Data Protection in China. in Belli L. & Gaspar W. Personal Data Architectures in the BRICS countries. (Oxford University Press 2025)

⁴¹ Idem.

⁴² Parsheera S. Stack is the New Black?: Evolution and Outcomes of the 'India-Stackification' Process. Computer Law & Security Review, 52 (2024) 105947

⁴³ Parsheera S. "Awaiting the Dawn of Data Protection Regulation in India" in Belli L. & Gaspar W. Personal Data Architectures in the BRICS countries. (Oxford University Press 2025)

Juntas, essas diversas experiências asiáticas revelam que a autodeterminação informativa sozinha fornece apenas uma explicação parcial da governança digital. A proteção dos direitos individuais continua importante, mas uma governança eficaz exige cada vez mais integrar privacidade com cibersegurança, infraestrutura tecnológica, política industrial e interoperabilidade técnica e jurídica. Nesse sentido, as experiências asiáticas contribuem significativamente para a evolução mais ampla de uma concepção individual de autodeterminação informativa para uma noção mais complexa de soberania dos dados.

1.3. UMA PERSPECTIVA AFRICANA: SOBERANIA DOS DADOS COMO RESISTÊNCIA AO COLONIALISMO DIGITAL

Se o constitucionalismo europeu enfatiza a autonomia individual e muitas abordagens asiáticas integram desenvolvimento com capacidade tecnológica, a pesquisa africana contribui com uma perspectiva diferente, mas igualmente importante, ao situar a governança de dados dentro da experiência histórica do colonialismo, dependência e participação desigual na economia política global.⁴⁴

O surgimento da economia digital gerou crescente preocupação de que padrões históricos de extração que caracterizam o domínio colonial possam ser reproduzidos por meio das tecnologias digitais contemporâneas.⁴⁵ Em vez de extrair recursos naturais, as potências coloniais e as multinacionais cada vez mais obtêm valor dos dados gerados por populações cujos países possuem capacidade limitada para governar, processar ou se beneficiar economicamente desses recursos. Esse fenômeno foi descrito por diversos estudiosos como colonialismo de dados⁴⁶, enfatizando a continuidade entre os sistemas históricos de extração econômica e o capitalismo digital contemporâneo.

Entre as contribuições mais influentes para esse debate está o trabalho de Everisto Benyera, que argumenta que a Quarta Revolução Industrial corre o risco de reproduzir relações coloniais por meio da concentração de infraestrutura tecnológica, propriedade intelectual, computação em nuvem, IA e capacidades de

⁴⁴ Veja notavelmente Benyera, E. *The Fourth Industrial Revolution and the Recolonisation of Africa: The Coloniality of Data*. (Routledge, 2021).

⁴⁵ Avila Pinto, R. (2018). Digital sovereignty or digital colonialism? New tensions of privacy, security and national policies. *SUR: International Journal on Human Rights*, 15(27), 15–27; Ricaurte, P. (2019). Data epistemologies, the coloniality of power, and resistance. *Television & New Media*, 20(4), 350-365; Nothias T, “An Intellectual History of Digital Colonialism” [2025] *The Journal of Communication*.

⁴⁶ Couldry, N., & Mejias, U. A. (2019). *The costs of connection: How data is colonizing human life and appropriating it for capitalism*. Stanford University Press.

processamento de dados fora do continente africano.⁴⁷ Nessa perspectiva, os dados tornam-se não apenas um objeto de regulação, mas um recurso estratégico cuja apropriação externa reforça a dependência estrutural.

A crítica africana, portanto, amplia o conceito de autodeterminação informativa em dois aspectos importantes. Primeiro, ela desvia a atenção dos direitos dos indivíduos para a agência de sociedades e Estados inteiros. Embora a privacidade pessoal continue sendo importante, a principal preocupação é se os países africanos possuem uma capacidade significativa para determinar como os dados gerados em suas economias contribuem para o desenvolvimento interno, em vez da acumulação externa de poder e riqueza. Questões relacionadas à localização de dados, infraestrutura de nuvem doméstica, mercados digitais regionais e capacidade tecnológica local adquirem assim uma importância para o desenvolvimento que vai além da lei convencional de privacidade.

Segundo, a pesquisa africana tem o mérito relevante de conectar explicitamente a governança digital com a justiça econômica.⁴⁸ O valor gerado por meio de modelos de negócios intensivos em dados está esmagadoramente concentrado em um número relativamente pequeno de empresas multinacionais de tecnologia com sede fora do continente. Consequentemente, as sociedades africanas contribuem com dados brutos enquanto capturam apenas uma pequena fração do valor econômico resultante. Essa assimetria reflete padrões históricos em que colônias exportavam matérias-primas enquanto a criação de valor industrial ocorria em outros lugares.⁴⁹

Essas preocupações têm informado cada vez mais iniciativas regionais, como o Quadro de Política de Dados da União Africana e esforços mais amplos para apoiar a transformação digital sob a Área de Livre Comércio Continental Africana (AfCFTA).⁵⁰ Em vez de defender a autarquia digital, essas iniciativas buscam fortalecer a capacidade regional por meio de marcos regulatórios comuns, mercados digitais interoperáveis e investimentos em infraestrutura digital. Soberania, portanto, é entendida como a capacidade de participar de forma mais equitativa da economia digital global, em vez de se retirar dela.

⁴⁷ Benyera, E. *The Fourth Industrial Revolution and the Recolonisation of Africa: The Coloniality of Data*. (Routledge, 2021).

⁴⁸ Folashadé Soulé, *Digital Sovereignty in Africa: Moving beyond Local Data Ownership* (CIGI Policy Brief No 185, Centre for International Governance Innovation, 25 June 2024)

⁴⁹ Idem.

⁵⁰ Kweku Adams, Rexford Attah-Boakye, Honglan Yu, Irene Chu and Dafydd Mali, 'African Continental Free Trade Area and Regional Trade in ICT and Digital Technologies' (2024) 30(4) *Journal of International Management*

Importante, a perspectiva africana introduz uma dimensão explícita de desenvolvimento que muitas vezes permaneceu implícita nos debates europeus sobre privacidade. Proteger informações pessoais, embora essencial, não garante por si só capacidade tecnológica, inovação doméstica ou transformação econômica. Um país pode adotar legislação sofisticada de proteção de dados enquanto permanece quase totalmente dependente de provedores de nuvem estrangeiros, ecossistemas de software, infraestruturas de pagamento e modelos de IA. Nessas circunstâncias, a lei de proteção de dados oferece apenas uma aparência formal de soberania, coexistindo com uma ordenação privada altamente eficaz definida por empresas privadas de tecnologia, tornando-se a forma mais eficaz de regulação, consagrando assim uma forma de soberania privada.⁵¹

A contribuição africana, portanto, reforça um dos argumentos centrais apresentados neste artigo: a soberania dos dados não pode ser reduzida apenas a direitos legais. Também exige capacidade institucional, capacidade tecnológica e estruturas econômicas capazes de gerar valor público a partir dos dados. Sem esses elementos complementares, a autodeterminação informativa corre o risco de se tornar um direito formalmente reconhecido cujo exercício prático permanece limitado pela dependência estrutural.

1.4. TRADIÇÕES CONVERGENTES, ÊNFASES DIVERGENTES

A análise comparativa desenvolvida acima demonstra que a autodeterminação informativa seguiu trajetórias históricas distintas em diferentes tradições jurídicas e políticas. Na Europa, o conceito surgiu principalmente como uma salvaguarda constitucional que protege a autonomia individual contra o processamento excessivo de dados. O sistema interamericano também fundamenta a autodeterminação informativa na dignidade humana, mas dá maior ênfase à participação democrática e à proteção da sociedade civil em contextos moldados por experiências autoritárias.

Muitas abordagens asiáticas, embora reconheçam cada vez mais a proteção de dados pessoais, integram a privacidade com objetivos mais amplos relacionados à segurança nacional, modernização tecnológica e desenvolvimento econômico. A pesquisa africana, por sua vez, introduz uma crítica pós-colonial que liga governança de dados à dependência, à extração desigual de valores e à justiça de desenvolvimento. Essas tradições diferem consideravelmente em suas prioridades normativas, arranjos institucionais e contextos políticos. No entanto, compartilham uma preocupação subjacente comum: preservar uma agência humana e coletiva significativa dentro de sociedades cada vez mais orientadas por dados.

⁵¹ Belli, L. Structural power as a critical element of digital platforms' private sovereignty. In E. Celeste, A. Heldt & C. Iglesias Keller (Eds.), *Constitutionalising social media* [pages]. (Hart, 2022).

Essa convergência é significativa porque sugere que o debate gradualmente passou da discussão sobre a necessidade de governança dos dados para a definição de como essa governança deve ser estruturada. Em cada região, os elementos centrais da autodeterminação informativa expandiram-se progressivamente além de um foco original na privacidade dos dados. As questões que os formuladores de políticas enfrentam hoje não se limitam mais a saber se os indivíduos devem controlar suas informações pessoais. Cada vez mais, elas dizem respeito à possibilidade de as sociedades possuírem capacidade institucional, tecnológica e econômica para governar a própria transformação digital.

É justamente nesse ponto que o conceito de soberania dos dados se torna necessário. A autodeterminação informativa continua sendo sua base normativa, mas aproveitar apenas sua dimensão individual não é mais suficiente para enquadrar os complexos desafios de governança gerados por IA, computação em nuvem, economias de plataforma, conflitos cibernéticos e infraestruturas digitais globais. Portanto, a soberania dos dados não deve ser entendida como substituindo a autodeterminação informativa. Na verdade, representa sua evolução lógica sob as condições da economia digital contemporânea e da geopolítica.

2. POR QUE UMA CONCEPÇÃO EXCLUSIVAMENTE INDIVIDUALISTA DA AUTODETERMINAÇÃO INFORMATIVA NÃO É MAIS SUFICIENTE

A análise comparativa desenvolvida na seção anterior demonstra que a autodeterminação informativa tornou-se uma pedra angular da governança digital contemporânea, refletindo um compromisso compartilhado com a preservação da autonomia humana em sociedades cada vez mais orientadas por dados. No entanto, a mesma análise comparativa também revela uma transformação mais sutil. Embora as *macrotenses* tradições jurídicas brevemente apresentadas acima comecem da proteção do indivíduo, nenhuma permanece restrita a uma compreensão exclusivamente individualista da governança digital.

Em diferentes jurisdições, preocupações relacionadas à segurança nacional, cibersegurança, dependências e capacidades tecnológicas, desenvolvimento econômico, política industrial e cooperação internacional têm progressivamente ampliado o escopo da regulação digital. Assim, a autodeterminação informativa continua a fornecer a base normativa, mas não esgota mais a gama de interesses implicados pela economia contemporânea de dados.

Essa evolução não é surpresa. A doutrina da autodeterminação informativa surgiu durante os estágios iniciais da informatização, quando as preocupações

constitucionais se concentravam principalmente na coleta e tratamento de informações pessoais por autoridades públicas. A Decisão do Censo Alemão foi decidida em uma era caracterizada por dinâmicas tecnológicas, econômicas e geopolíticas radicalmente diferentes das atuais. Naquela época, os dados pessoais constituíam o principal objeto de regulação, e a principal questão constitucional dizia respeito à relação entre o indivíduo e o Estado.

O ambiente tecnológico passou por uma transformação profunda desde então. Os dados tornaram-se não apenas objetos de proteção legal, mas também ativos econômicos estratégicos, insumos essenciais para sistemas de IA, bases de serviços públicos digitais, impulsionadores da inovação industrial e, cada vez mais, instrumentos de influência geopolítica. Igualmente importante, as infraestruturas digitais adquiriram importância estratégica, cuja governança afeta diretamente a resiliência nacional e a competitividade econômica. Nessas condições, uma concepção exclusivamente individualista de autodeterminação informativa torna-se insuficiente por pelo menos três razões.

Primeiro, visa regular apenas uma dimensão de ecossistemas digitais cada vez mais complexos. A lei de proteção de dados tem como principal alvo – não necessariamente de forma eficaz⁵² – a relação entre os indivíduos e aqueles que processam suas informações pessoais. As garantias que estabelece continuam sendo indispensáveis para proteger a autonomia individual. No entanto, eles não determinam quem possui, opera e pode extrair valor das infraestruturas em nuvem nem sob quais condições, quem desenvolve e tem acesso a modelos fundamentais de IA, quem controla os sistemas digitais de pagamento ou como o valor gerado por atividades intensivas em dados é redistribuído. Questões relacionadas à capacidade tecnológica, estrutura de mercado, desenvolvimento industrial e tributação de dados permanecem em grande parte fora do escopo do direito clássico de privacidade.⁵³

Segundo, uma concepção individualista aborda inadequadamente a natureza coletiva de muitos riscos digitais contemporâneos.⁵⁴ A cibersegurança talvez seja o

⁵² David Erdos, 'Acontextual and Ineffective? Reviewing the GDPR Two Years On' (International Forum for Responsible Media, 2020); Ryan, J. 'Europe's Governments Are Failing the GDPR: Brave's 2020 Report on the Enforcement Capacity of Data Protection Authorities' (2020); Karjalainen, T. 'The Battle of Power: Enforcing Data Protection Law against Companies Holding Data Power' (2022) 47 Computer Law & Security Review 105742.

⁵³ Belli L., Fossati G. McClaskey L. and Zingales, N. Proteção, Tributação e Equidade de Dados: Equilibrando Valores, Riscos e Obrigações na Economia Digital. (Lumen Juris 2026)

⁵⁴ Belli L. and others, Soberania Digital e Inteligência Artificial no Brasil: Rumo à autonomia tecnológica (Lumen-Juris 2026); Belli, L. and Bhinder, A. Cooperative Digital Sovereignty and Artificial Intelligence

exemplo mais claro. Um ataque cibernético bem-sucedido que comprometa a confidencialidade, integridade e disponibilidade de um sistema nacional de pagamento, uma rede elétrica ou um serviço público digital governamental pode comprometer a segurança e autonomia de milhões de indivíduos simultaneamente, independentemente de seus dados pessoais terem sido processados legalmente sob a legislação de privacidade aplicável. Da mesma forma, a dependência de provedores de nuvem estrangeiros sujeitos à jurisdição estrangeira cria riscos sistêmicos de continuidade do serviço que não podem ser resolvidos apenas por consentimento individual ou direitos de proteção de dados. De fato, a resiliência e a segurança dos ecossistemas digitais tornaram-se um bem público que exige governança coletiva.⁵⁵

Terceiro, uma perspectiva individual sobre a autodeterminação informativa diz relativamente pouco sobre a economia política dos dados. A extraordinária concentração dos mercados digitais entre um número limitado de empresas globais de tecnologia gerou assimetrias sem precedentes em poder econômico, capacidade tecnológica e controle sobre infraestruturas digitais. Essas assimetrias afetam não apenas a concorrência, mas também a capacidade dos Estados de buscar políticas digitais independentes, fomentar a inovação doméstica e garantir que o valor gerado pelos dados contribua para o desenvolvimento sustentável e inclusivo. Sob essa perspectiva, a soberania diz respeito não apenas à proteção dos indivíduos, mas também à sustentabilidade dos mercados, infraestruturas nacionais e sistemas de inovação.

Em conjunto, esses desenvolvimentos sugerem que o desafio contemporâneo não é mais apenas proteger os indivíduos do processamento excessivo de dados. É garantir que as sociedades possuam a capacidade institucional para governar a transformação digital por si mesmas. Portanto, embora forneça a base conceitual e constitucional sobre a qual uma concepção mais ampla de soberania de dados deve ser construída, uma concepção meramente individualista da autodeterminação informativa continua sendo insuficiente para assegurar aquilo que buscamos definir como soberania de dados, ou seja, a capacidade de entender como funcionam as tecnologias de processamento de dados, desenvolver alternativas e regulá-las de forma eficaz.

Essa concepção mais ampla não abandona o indivíduo. Pelo contrário, busca preservar a autonomia individual ao reconhecer que essa autonomia depende cada vez mais de condições que vão muito além da lei de privacidade de dados. A

Promoting Resilience, Strategic Openness, and Self-Determination. (Digital Cooperation Organization, 2026).

⁵⁵ DeNardis, L. (2020). *The internet in everything: Freedom and security in a world with no off switch*. Yale University Press

autodeterminação informativa significativa hoje pressupõe infraestruturas digitais seguras, mercados competitivos, arquiteturas tecnológicas confiáveis, infraestruturas ciberseguras, instituições públicas resilientes e participação equitativa no valor econômico gerado pelos dados. Os direitos individuais e a governança coletiva, portanto, não devem ser vistos como objetivos concorrentes, mas como componentes mutuamente reforçadores do mesmo projeto constitucional.

A transição da autodeterminação informativa para a soberania dos dados deve, portanto, ser entendida como análoga a desenvolvimentos anteriores na teoria constitucional. Constituições liberais surgiram inicialmente para proteger indivíduos contra poderes governamentais arbitrários. Com o tempo, porém, a governança constitucional expandiu-se para incluir direitos sociais, regulação econômica, administração pública e responsabilidade institucional, refletindo a crescente complexidade das sociedades modernas.⁵⁶

A evolução da governança digital segue uma trajetória semelhante. A autodeterminação informativa continua sendo seu núcleo constitucional, mas as sociedades digitais contemporâneas exigem um arcabouço de governança mais amplo capaz de integrar direitos, inovação tecnológica, (ciber)tecnologia, segurança, desenvolvimento econômico e responsabilidade democrática. É essa estrutura multidimensional de governança que este artigo descreve como soberania de dados.

3. AS DIMENSÕES CONSTITUTIVAS DA SOBERANIA DOS DADOS

A seção anterior argumentava que a autodeterminação informativa continua sendo a base normativa indispensável da governança digital, mas que ela já não é suficiente para enfrentar as transformações estruturais produzidas pela economia contemporânea de dados, dependências digitais e tensões geopolíticas. Embora os direitos individuais continuem sendo essenciais, é excessivamente otimista ou ingênuo supor que, sozinhos, eles podem determinar efetivamente como a autoridade pública, infraestruturas tecnológicas, mercados e instituições devem ser organizados. A questão central, portanto, não é mais apenas como os indivíduos podem exercer controle sobre informações pessoais, mas como as sociedades democráticas podem desenvolver as capacidades institucionais necessárias para governar a transformação digital no interesse público.

⁵⁶ Katharine G. Young, *Constituting Economic and Social Rights* (Oxford: Oxford University Press, 2012).

Esta seção desenvolve a proposição teórica central do artigo de que a soberania dos dados não deve ser entendida apenas como um princípio jurídico único, um objetivo tecnológico ou um instrumento político alcançável apenas por meio da localização de dados, infraestrutura doméstica ou legislação de privacidade mais forte, mas é melhor entendida como uma capacidade institucional integrada gerada pela interação de múltiplas dimensões de governança. Cada dimensão aborda uma fonte distinta de vulnerabilidade dentro dos ecossistemas digitais, mas nenhuma é suficiente isoladamente. A soberania surge apenas quando essas capacidades se reforçam mutuamente e permitem que estados e sociedades exerçam controle significativa sobre as condições legais, tecnológicas, econômicas e organizacionais pelas quais os dados são gerados, extraídos, trocados e transformados em valor.⁵⁷

Com base nesse entendimento, a seção identifica seis dimensões constitutivas da soberania dos dados: (I) proteção de dados; (II) cibersegurança e resiliência digital; (III) infraestrutura pública digital; (IV) desenvolvimento industrial e capacidade tecnológica; (V) competição e inovação; e (VI) justiça fiscal. Cabe destacar que, essas dimensões não devem ser interpretadas como setores políticos isolados, mas como capacidades institucionais complementares por meio das quais a agência soberana é progressivamente construída e sustentada.

Essa perspectiva multidimensional também reflete a crescente complexidade da própria governança da informação. A proteção de dados sem infraestruturas resilientes não pode preservar a confiança. A cibersegurança sem governança responsável não pode garantir legitimidade. Infraestrutura pública digital sem capacidade tecnológica não pode garantir autonomia de longo prazo. A política industrial sem mercados competitivos pode reforçar a concentração em vez da inovação, enquanto a capacidade fiscal determina, em última instância, se esses arranjos de governança podem ser mantidos e adaptados ao longo do tempo. A eficácia de cada dimensão, portanto, depende das outras. Portanto, a soberania dos dados é melhor compreendida como um sistema institucional do que como uma lista de verificação regulatória.

Essa compreensão representa uma importante ruptura com grande parte da literatura existente, que frequentemente aborda a soberania dos dados por meio de instrumentos políticos isolados ou arranjos de governança específicos de setores. O arcabouço proposto aqui, em vez disso, concebe a soberania como uma capacidade institucional emergente cuja eficácia depende da coerência dos arranjos

⁵⁷ Cohen, J.E. *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford University Press 2019); Zuboff, S. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Public Affairs 2019).

constitucionais, tecnológicos, desenvolvimentistas, econômicos e de governança que operam ao longo da pilha digital.

As subseções seguintes examinam cada dimensão constitutiva individualmente antes de retornar, na Seção 3.7, para demonstrar como sua interação deve ser vista como a base de um quadro integrado de governança. O objetivo desta apresentação progressiva é preservar a especificidade analítica de cada dimensão, ao mesmo tempo em que mostra que a soberania dos dados emerge, em última análise, não de nenhum componente individual, mas da coerência da arquitetura institucional que os conecta.

3.1. PROTEÇÃO DE DADOS

A primeira dimensão constitutiva da soberania dos dados é a proteção de dados, que funciona como o ponto de entrada normativo da governança digital soberana. Ela fornece a legitimidade constitucional de que todo sistema de governança de dados depende, em última instância, porque a autoridade pública não pode ser exercida legitimamente em sociedades baseadas em dados a menos que os indivíduos possam confiar que informações pessoais são coletadas, processadas, compartilhadas e mantidas de acordo com legalidade, justiça, transparência, responsabilidade e supervisão eficaz.⁵⁸

Portanto, a importância constitucional da proteção de dados vai além da privacidade. Os dados pessoais cada vez mais mediam, cada vez mais, o acesso ao emprego, educação, saúde, serviços financeiros, proteção social e participação democrática. Decisões sobre elegibilidade, identidade, crédito, mobilidade, benefícios públicos e expressão política são cada vez mais moldadas por sistemas automatizados que operam com processamento de dados em larga escala. Proteger a autodeterminação informativa, portanto, salvaguarda não apenas a autonomia pessoal, mas também as condições necessárias para a igualdade democrática, a dignidade humana e o Estado de Direito em sociedades cada vez mais algorítmicas. Como estabelece o artigo 1 da Loi Informatique et Libertés francesa de 1978:

"A tecnologia da informação deve estar a serviço de todos os cidadãos. Seu desenvolvimento deverá ocorrer no contexto da cooperação internacional. Não violará a identidade humana, os

⁵⁸ Brian Nogrèrès, A. (2022). Principles underpinning privacy and the protection of personal data (UN Doc. A/77/196). United Nations, General Assembly, Brian Nogrèrès, A. (2023). *Principles of transparency and explainability in the processing of personal data* (UN Doc. A/78/310). United Nations, General Assembly.

direitos humanos, a privacidade, nem as liberdades individuais ou públicas"

Esse princípio é tão fundamental que foi incorporado como um dos pilares da proposta Convenção de Interamericana sobre Autodeterminação Informativa, o Tratamento e Circulação de Dados Pessoais.⁵⁹ No entanto, a proteção de dados não deve ser entendida apenas como um mecanismo defensivo projetado para restringir o poder público ou privado. Frameworks de proteção de dados bem projetados também desempenham uma função habilitadora. Ao estabelecer regras legais previsíveis, alocar responsabilidades institucionais e criar condições confiáveis para o compartilhamento legal de dados, eles facilitam a inovação, a pesquisa científica, a administração pública eficiente e a transformação digital responsável.⁶⁰ A proteção de dados, portanto, cria a base da segurança jurídica e da confiança institucional necessárias para uma governança legítima de dados.

Essa distinção é particularmente importante dentro do quadro proposto neste artigo. A governança de dados frequentemente exige a circulação legal de informações através das fronteiras institucionais, seja para fornecer serviços públicos, apoiar DPI, viabilizar sistemas governamentais interoperáveis ou fomentar a inovação orientada por dados.⁶¹ Para que as salvaguardas de autodeterminação informativa sejam significativas, a proteção de dados também exige garantias institucionais sólidas. Autoridades supervisoras independentes, direitos executáveis, recursos acessíveis⁶², poderes de auditoria e sanções eficazes transformam princípios abstratos em restrições práticas ao poder governamental e corporativo. Sem tais mecanismos, a proteção de dados corre o risco de se tornar um compromisso formal, em vez de uma fonte duradoura de legitimidade dentro da arquitetura mais ampla da soberania dos dados.

Por essa razão, argumentamos que a proteção de dados constitui um pilar fundamental da soberania dos dados, e não sua expressão completa. Estabelece a legitimidade pela qual a autoridade sobre dados pessoais pode ser exercida, mas não determina, por si só, quem governa infraestruturas digitais críticas, quem controla as capacidades tecnológicas estratégicas, como os ecossistemas

⁵⁹ Luca Belli, Ana Brian Nougères, Jonathan Mendoza Iserte, Pablo Andrés Palazzi and Nelson Remolina Angarita, *Transferência Internacional de Dados Pessoais na América Latina: Rumo à Harmonização de Normas* (1st edn, Lumen Juris 2024), Annex A.

⁶⁰ UNCTAD. Cross-border data flows and development: For whom the data flow. Digital Economy Report 2021.

⁶¹ Richard Pope, *Platformland: An Anatomy of Next-Generation Public Services* (London: London Publishing Partnership, 2025), 27-45.

⁶² Brian Nougères, A. (2024). *Legal safeguards for personal data protection and privacy in the digital age* (UN Doc. A/HRC/55/46). United Nations, Human Rights Council.

interoperáveis são organizados ou se os Estados possuem capacidade prática para exercer uma agência significativa dentro da economia digital.

A autodeterminação informativa, portanto, continua sendo indispensável, mas deve ser complementada pelas capacidades institucionais adicionais desenvolvidas ao longo do restante deste capítulo. A soberania dos dados começa com direitos, mas é realizada por meio da governança. No entanto, os direitos permanecem eficazes apenas se as infraestruturas pelas quais são exercidos permanecerem confiáveis e resilientes. A proteção de dados, portanto, estabelece a legitimidade normativa da soberania dos dados, enquanto a cibersegurança preserva as condições operacionais sob as quais essa legitimidade pode ser alcançada.

3.2. CIBERSEGURANÇA E CIBERRESILIÊNCIA

A segunda dimensão constitutiva é a cibersegurança. Discussões tradicionais sobre autodeterminação informativa geralmente assumem que direitos legais podem ser exercidos de forma significativa uma vez estabelecidas regras apropriadas que regem o processamento de dados. Ecossistemas digitais contemporâneos desafiam essa suposição porque os direitos legais se tornam ineficazes sempre que as infraestruturas digitais são comprometidas.

Estruturas recentes de proteção de dados e cibersegurança parecem reconhecer essa limitação, promovendo a Segurança por Design como princípio central – ou até mesmo "um mantra aspiracional"⁶³ – que exige a consideração das necessidades de segurança dos sistemas antes e a integração dessas necessidades no projeto e construção subsequentes dos sistemas.

Portanto, a cibersegurança transforma a soberania de um conceito puramente jurídico em uma questão de resiliência operacional.⁶⁴ Um governo pode adotar legislação exemplar de privacidade enquanto seus bancos de dados e infraestrutura digital permanecem vulneráveis a ataques de ransomware. Cidadãos podem desfrutar de amplas proteções legais em relação às suas informações pessoais, mas essas proteções se tornam em grande parte ilusórias se atores hostis conseguirem exfiltrar informações sensíveis por meio de vulnerabilidades de software ou comprometer infraestruturas digitais críticas por meio de operações cibernéticas.⁶⁵

⁶³ Bygrave L.A. Security by Design: Aspirations and Realities in a Regulatory Context. Oslo Law Review. Volume 8, No. 3-2021, p. 126–177.

⁶⁴ Belli, L. et al. Governança e regulação da cibersegurança no Brasil: proteção da infraestrutura crítica, segurança da informação e construção da soberania digital. (Lumen Juris, 2025); Belli, L. et al. Cibersegurança: uma visão sistêmica rumo a uma Proposta de Marco Regulatório para um Brasil Digitalmente soberano. Rio de Janeiro, RJ: FGV Direito Rio, 2023.

⁶⁵ Idem.

A crescente digitalização da administração pública reforça ainda mais essa relação. Sistemas tributários, registros eleitorais, registros de saúde, programas de proteção social, sistemas de pagamento e infraestruturas de identidade agora dependem de redes digitais interconectadas cuja interrupção pode prejudicar significativamente a capacidade dos governos de desempenhar suas funções mais básicas. Consequentemente, a cibersegurança se assemelha cada vez mais à defesa nacional: protege não apenas a informação, mas também a continuidade institucional do próprio Estado.⁶⁶

Essa observação tem importantes implicações conceituais. A soberania dos dados não pode simplesmente limitar-se ao controle sobre esses; também deve englobar a capacidade de preservar a integridade, disponibilidade e confidencialidade dos ecossistemas digitais. A segurança, portanto, não é um pré-requisito externo para a soberania, mas uma de suas dimensões constitutivas.

A cibersegurança abrange as políticas, instituições, tecnologias e capacidades operacionais necessárias para proteger ativos digitais, sistemas, redes e os indivíduos que deles dependem contra ameaças cibernéticas. Cada vez mais, esse conceito é complementado pelo de ciberresiliência, ou seja, a capacidade dos sistemas digitais não apenas de prevenir e resistir a incidentes cibernéticos, mas também de se recuperar rapidamente e continuar operando sob condições adversas.⁶⁷ Juntas, cibersegurança e ciberresiliência fornecem as condições institucionais necessárias para o exercício da soberania no ambiente digital.

Essa relação reflete uma transformação mais ampla na natureza dos dados. Os dados não são mais meros objetos de proteção legal; eles se tornaram ativos estratégicos que sustentam a administração pública, atividade econômica, pesquisa científica, infraestrutura crítica e segurança nacional. Sob a perspectiva proposta neste artigo, a soberania dos dados vai, portanto, além da própria governança dos dados para abranger a segurança dos ecossistemas digitais que os sustentam. A soberania hoje depende não apenas da autoridade legal para regular o processamento de dados, mas também da capacidade de preservar a confidencialidade, integridade e disponibilidade (conhecidas como "tríade da CIA") das infraestruturas que sustentam a sociedade digital. Data centers, plataformas de computação em nuvem, redes de telecomunicações, cabos submarinos e outras infraestruturas digitais tornaram-se críticos, pois a disrupção pode comprometer a continuidade do governo, a estabilidade econômica e as instituições democráticas.

⁶⁶ Idem.

⁶⁷ International Organization for Standardization, *ISO 22316:2017 Security and Resilience—Organizational Resilience—Principles and Attributes* (ISO 2017); National Institute of Standards and Technology, *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach* (NIST Special Publication 800-160 vol 2 rev 1, 2021); Richard A Caralli, Julia H Allen, David W White and others, *CERT® Resilience Management Model (CERT®-RMM): A Maturity Model for Managing Operational Resilience* (Version 1.2, CMU/SEI-2016-TR-012, Carnegie Mellon University Software Engineering Institute 2016)

Portanto, essa evolução altera a relação entre cibersegurança e direitos fundamentais. Autodeterminação informativa, privacidade, liberdade de expressão, acesso a serviços públicos e participação democrática dependem cada vez mais de infraestruturas digitais seguras. De fato, o direito legal à proteção de dados oferece proteção prática limitada se informações pessoais puderem ser exfiltradas por meio de ataques cibernéticos, manipuladas por agentes maliciosos ou tornadas inacessíveis por ransomware. A cibersegurança deve, portanto, ser entendida não apenas como um instrumento de segurança nacional, mas também como uma obrigação positiva do Estado de criar as condições sob as quais direitos fundamentais possam ser exercidos de forma eficaz.⁶⁸

Importa destacar que a complementaridade entre cibersegurança e governança de dados vai além da proteção. Investimentos em pesquisa, desenvolvimento tecnológico e capacidades digitais contribuem simultaneamente para uma cibersegurança mais forte e uma regulamentação mais eficaz. Regulação, inovação tecnológica e capacidade operacional devem, portanto, ser entendidas como componentes mutuamente reforçadores do mesmo ecossistema de governança. Assim, as estratégias nacionais de cibersegurança devem perseguir múltiplos objetivos simultaneamente. Essas estratégias devem fortalecer a proteção dos cidadãos e das instituições públicas, aumentar a resiliência econômica, fomentar a capacidade tecnológica e apoiar o desenvolvimento digital sustentável.⁶⁹ Alcançar esses objetivos exige ação coordenada entre governo, indústria, academia e sociedade civil, refletindo a natureza inerentemente multidisciplinar da governança da cibersegurança.

Tais estratégias devem englobar vários elementos complementares, incluindo o estabelecimento de padrões mínimos de cibersegurança; a proteção da infraestrutura crítica de informação e dos serviços essenciais; o desenvolvimento de capacidades nacionais para monitoramento, prevenção e resposta a incidentes cibernéticos; responsabilidades institucionais claras para supervisão e fiscalização regulatória; mecanismos para compartilhamento de informações e coordenação operacional entre autoridades públicas e operadores privados; investimento em pesquisa em cibersegurança e desenvolvimento de força de trabalho; e suporte a tecnologias digitais confiáveis capazes de reduzir vulnerabilidades estratégicas enquanto permanecem interoperáveis com sistemas internacionais.⁷⁰

⁶⁸ Belli, L. et al. Governança e regulação da cibersegurança no Brasil: proteção da infraestrutura crítica, segurança da informação e construção da soberania digital. (Lumen Juris, 2025); Belli, L. et al. Cibersegurança: uma visão sistêmica rumo a uma Proposta de Marco Regulatório para um Brasil Digitalmente soberano. Rio de Janeiro, RJ: FGV Direito Rio, 2023.

⁶⁹ Idem.

⁷⁰ Belli L. and others, Soberania Digital e Inteligência Artificial no Brasil: Rumo à autonomia tecnológica (Lumen-Juris 2026).

A crescente importância estratégica da cibersegurança também reforça a necessidade de reduzir a dependência tecnológica excessiva em setores críticos. Embora nenhum país possa realisticamente alcançar autonomia tecnológica completa, a dependência excessiva de infraestruturas digitais externas, serviços em nuvem ou ecossistemas de software pode expor funções públicas essenciais a vulnerabilidades estratégicas além do controle direto das autoridades nacionais. Portanto, construir capacidade em cibersegurança exige não apenas expertise técnica, mas também investimentos em infraestrutura digital confiável, cadeias de suprimentos resilientes e ecossistemas tecnológicos diversificados capazes de apoiar a continuidade dos serviços públicos essenciais.

Ao mesmo tempo, a cibersegurança ilustra por que a soberania dos dados não pode ser buscada por meio do isolamento. Ecossistemas digitais são inerentemente interconectados, e ameaças cibernéticas rotineiramente transcendem fronteiras nacionais. Vulnerabilidades que afetam softwares, serviços em nuvem, infraestrutura de telecomunicações ou cadeias de suprimentos frequentemente geram efeitos em cascata em múltiplas jurisdições. A cibersegurança eficaz, portanto, depende da cooperação internacional em áreas como cibercrime, resposta a incidentes, inteligência de ameaças, padrões técnicos e proteção de infraestrutura crítica.

Em última análise, cibersegurança e ciberresiliência não são simplesmente políticas de apoio dentro do quadro mais amplo da soberania dos dados. Elas constituem capacidades indispensáveis de governança sem as quais nenhuma das outras dimensões da soberania dos dados pode ser efetivamente realizada. Assim, a cibersegurança amplia o alcance da autodeterminação informática de proteger a autonomia individual para salvaguardar as condições institucionais sob as quais a autonomia pode ser exercida. A segurança, no entanto, sozinha não determina como a autoridade pública digital é exercida. Uma vez que infraestruturas resilientes existam, a próxima questão diz respeito a como elas devem ser organizadas para cumprir funções públicas e coordenar a governança de dados. Esse é o papel da infraestrutura pública digital.

3.3. INFRAESTRUTURA PÚBLICA DIGITAL

Se a cibersegurança preservar a integridade, disponibilidade e resiliência dos ecossistemas digitais, a infraestrutura pública digital (DPI) determina se esses ecossistemas seguros podem ser usados para operacionalizar a autoridade pública, entregar direitos e serviços e coordenar a governança de dados na prática. A segurança protege as condições sob as quais a autonomia pode ser exercida, enquanto a DPI fornece a arquitetura institucional e tecnológica pela qual essa autonomia se torna administrativamente eficaz, socialmente acessível e democraticamente responsável.

A DPI contribui para a soberania dos dados porque visa operacionalizar a governança dos dados por meio de sistemas que permanecem responsáveis, interoperáveis, seguros e controláveis democraticamente. Uma das características definidoras da governança digital contemporânea é que a autoridade pública depende cada vez mais não apenas de regras legais, mas também das infraestruturas pelas quais essas regras se tornam eficazes. A legislação de proteção de dados, o direito administrativo, a proteção do consumidor, o direito da concorrência, a regulamentação de cibersegurança e a governança setorial continuam sendo fundamentos indispensáveis do estado digital. Sua eficácia prática, no entanto, depende do design e da governança dos sistemas pelos quais as identidades são estabelecidas, as transações são executadas, as informações são trocadas e o acesso aos serviços públicos é organizado.

Portanto, a DPI deve ser entendida como mais do que um conjunto de tecnologias digitais, aplicações ou plataformas governamentais. Trabalhos recentes de políticas públicas e acadêmicos descrevem a DPI como capacidades compartilhadas, fundamentais e interoperáveis, capazes de apoiar múltiplos serviços públicos e privados em escala social. Este artigo se baseia nesse entendimento enquanto avança uma proposta institucional mais ampla: a DPI é pública não apenas porque é acessível ou financiado publicamente, mas porque cria as condições tecnológicas e institucionais pelas quais a autoridade pública pode ser exercida, coordenada, restringida e responsabilizada dentro dos serviços digitais.⁷¹

Essa interpretação esclarece o que torna tal infraestrutura genuinamente pública. Infraestruturas digitais não são arranjos neutros: seu design e governança incorporam direções, distribuem valor e moldam relações entre instituições públicas, atores privados e a sociedade.⁷² O caráter público da DPI, portanto, não pode ser inferido apenas da propriedade governamental, do financiamento público ou da disponibilidade universal. Depende se a infraestrutura persegue propósitos públicos democráticos definidos, gera valor público amplamente compartilhado e permanece responsável perante as instituições e comunidades afetadas por ela.⁷³

⁷¹ Ole Hanseth and Kalle Lyytinen, 'Design Theory for Dynamic Complexity in Information Infrastructures' (2010) *Journal of Information Technology*; OECD, *Digital Public Infrastructure for Digital Governments* (OECD Public Governance Policy Papers No 68, OECD Publishing 2024) ; David Eaves and Krisstina Rao, *Digital Public Infrastructure: A Framework for Conceptualisation and Measurement* (UCL Institute for Innovation and Public Purpose Working Paper 2025).

⁷² Brett Frischmann, *Infrastructure: The Social Value of Shared Resources* (Oxford University Press 2012).

⁷³ Idem.

Publicidade, portanto, é uma qualidade institucional, e não uma simples classificação de propriedade. Uma plataforma de propriedade governamental pode minar a soberania se depender de componentes proprietários opacos, fornecedores insubstituíveis ou acordos contratuais que impeçam auditorias, modificações ou migrações. Por outro lado, componentes desenvolvidos privadamente ou de código aberto podem contribuir para a infraestrutura pública, onde permanecem interoperáveis, contestáveis, portáteis e sujeitos a uma governança pública eficaz. As questões relevantes não se limitam a quem é o dono dos servidores ou softwares, mas incluem quem define os propósitos da infraestrutura, quem controla padrões e interfaces, quem autoriza o acesso, quem assume a responsabilidade por falhas e se as instituições democráticas mantêm a capacidade de alterar sua direção tecnológica.

A DPI pode, portanto, ser descrita como arquitetura constitucional em um sentido funcional. Não é constitucional porque substitui o direito constitucional, nem porque o design técnico pode se tornar a fonte autônoma de legitimidade. Na verdade, é constitucional porque estrutura como a autoridade legalmente constituída é implementada e vivida na prática. Essa percepção estende a proposição de Lessig de que a arquitetura constitui uma modalidade de regulação, permanecendo consistente com o alerta de Hildebrandt de que o design tecnológico não pode substituir o Estado de Direito.⁷⁴ A DPI deve tornar os princípios legais tecnicamente eficazes, preservando os controles institucionais, a abertura interpretativa, o devido processo, a revisão judicial e a responsabilidade democrática.

A importância institucional da DPI está na transição de aplicações isoladas para capacidades públicas reutilizáveis. Os governos tradicionalmente desenvolveram serviços digitais em silos organizacionais, reconstruindo repetidamente funções como verificação de identidade, autenticação, pagamentos, notificações, troca de documentos e gestão de registros. A literatura do Governo como Plataforma⁷⁵ mostra como componentes comuns, dados e interfaces podem reduzir duplicações e apoiar o desenvolvimento de serviços no setor público. A DPI se baseia nessa lógica

⁷⁴ Lessig, L. 'The Law of the Horse: What Cyberlaw Might Teach' (1999) 113(2) Harvard Law Review 501;

Lessig, L. Code: Version 2.0 (Basic Books 2006); Mireille Hildebrandt, 'Algorithmic Regulation and the Rule of Law' (2018) 376(2128) *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 20170355

⁷⁵ Tim O'Reilly, 'Government as a Platform' in Daniel Lathrop and Laurel Ruma (eds), *Open Government: Collaboration, Transparency, and Participation in Practice* (O'Reilly Media 2010) 11–40; Helen Margetts and André Naumann, *Government as a Platform: What Can Estonia Show the World?* (Oxford Internet Institute, University of Oxford 2017).

de plataforma, mas vai além da eficiência administrativa: identidade compartilhada, pagamento, troca de dados, credencial e capacidades de confiança moldam a distribuição de autoridade, responsabilidade e acesso pela sociedade.

Exemplos concretos ilustram essa função constitucional. Os sistemas de identidade digital influenciam quem pode ser reconhecido por instituições públicas, quais atributos os indivíduos devem revelar, como direitos e benefícios são comprovados e se erros podem ser contestados. Infraestruturas de pagamento como a Pix do Brasil ou a UPI da Índia afetam a inclusão financeira, transferências públicas, concorrência e a relação entre autoridades públicas e atores financeiros regulados. Estruturas confiáveis de troca de dados, como a X-Road da Estônia, e sistemas emergentes de credenciais digitais, como a Carteira de Identidade Digital da UE, também permitem que afirmações autoritativas circulem e sejam reconhecidas através das fronteiras institucionais. Sua importância não reside apenas na conveniência ou eficiência, mas nas condições institucionais que criam para reconhecimento, participação e responsabilidade.

Essas capacidades compartilhadas expandem o que Mann descreve como o poder infraestrutural do Estado: a capacidade das instituições públicas de coordenar atividades sociais e administrativas por meio de arranjos duradouros que se estendem por toda a sociedade.⁷⁶ Assim, a DPI pode aumentar a capacidade dos governos de identificar necessidades, entregar benefícios, verificar obrigações e coordenar ações públicas. No entanto, o poder infraestrutural é normativamente ambivalente. A mesma capacidade que permite uma prestação de serviços mais eficaz também pode possibilitar vigilância, exclusão, controle automatizado ou a rápida propagação de erros administrativos. A questão constitucional, portanto, não é se o Estado deve possuir capacidade infraestrutural, mas como essa capacidade é distribuída, governada e limitada.

Um modelo federado e policêntrico oferece um meio de conciliar capacidade infraestrutural com autoridade distribuída. Baseando-se no trabalho de Ostrom⁷⁷, a DPI pode ser entendida como um arranjo no qual múltiplas instituições autônomas exercem responsabilidade dentro de seus respectivos domínios, cooperando sob regras compartilhadas. Registros civis, administrações fiscais, autoridades de saúde,

⁷⁶ Mann, M. (1984). The autonomous power of the state: Its origins, mechanisms and results. *European Journal of Sociology / Archives Européennes de Sociologie*, 25(2), 185–213

⁷⁷ Por exemplo, Ostrom, Elinor. "Beyond Markets and States: Polycentric Governance of Complex Economic Systems." *American Economic Review* 100, no. 3 (2010): 641-672. Ostrom, Elinor. "Polycentric Systems for Coping with Collective Action and Global Environmental Change." *Global Environmental Change* 20, no. 4 (2010): 550-557. Ostrom, Elinor. *Understanding Institutional Diversity*. Princeton: Princeton University Press, 2005.

instituições educacionais, bancos centrais e outros órgãos públicos podem permanecer autoritativos para os registros e funções legalmente confiados a eles, enquanto a infraestrutura compartilhada permite a cooperação sem transferir todos os dados ou autoridade de tomada de decisão para uma única plataforma central. Tal federação, no entanto, exige padrões comuns, definições semânticas, estruturas de garantia, controles de identidade e acesso, regras de auditoria e processos para resolver inconsistências.

A governança de dados constitui a camada constitucional que define autoridade institucional, fins legais para o processamento de dados, condições de acesso e reutilização, padrões de qualidade e mecanismos de supervisão e reparação. A DPI operacionaliza esses arranjos legais e institucionais por meio da arquitetura tecnológica, mas não cria autoridade legal por si só. De fato, a colaboração confiável de dados entre instituições públicas, atores privados e sociedade civil depende de propósitos claramente definidos, acesso diferenciado e mecanismos robustos de responsabilização.

Como a DPI media o exercício da autoridade pública, as salvaguardas constitucionais devem ser incorporadas por design. Princípios como limitação de propósito, proporcionalidade e minimização de dados devem reger a troca de dados, enquanto tecnologias como divulgação seletiva, credenciais verificáveis, controles de acesso baseados em funções e registros de auditoria à prova de adulteração podem fortalecer a privacidade e a responsabilidade.⁷⁸ A supervisão humana, procedimentos correccionais acessíveis, soluções eficazes e a prestação inclusiva de serviços – incluindo alternativas significativas e não digitais – continuam essenciais para preservar o devido processo e o acesso igualitário.⁷⁹

Ao mesmo tempo, DPI mal regulado pode gerar novos riscos.⁸⁰ Centralização excessiva pode facilitar a vigilância, o aumento de funções, a exclusão automatizada e falhas sistêmicas, enquanto a interoperabilidade pode expandir o acesso a dados sensíveis além de propósitos legítimos. Assim, a soberania dos dados exige a capacidade institucional de auditar, modificar e substituir infraestrutura digital. Devidamente governada, a DPI torna-se um componente constitucional da soberania dos dados: uma arquitetura institucional interoperável, segura e responsável que fortalece a autoridade pública enquanto preserva a autonomia institucional, a responsabilidade democrática e os direitos fundamentais. Sua

⁷⁸ Hannah Draper, and others. *A Consumer-centric Approach to Digital Public Infrastructure for Sustainable Financial Inclusion* (T20 Brasil Policy Brief, Task Force 5, 2024)

⁷⁹ Brian Nougères, A. (2024). *Legal safeguards for personal data protection and privacy in the digital age* (UN Doc. A/HRC/55/46). United Nations, Human Rights Council.

⁸⁰ Idem.

sustentabilidade a longo prazo, no entanto, depende, em última análise, das capacidades tecnológicas e industriais domésticas capazes de desenvolver, manter e melhorar continuamente infraestruturas digitais essenciais.

3.4. DESENVOLVIMENTO INDUSTRIAL E CAPACIDADE TECNOLÓGICA

O desenvolvimento industrial constitui uma dimensão indispensável da soberania dos dados porque a governança depende, em última instância, não apenas da autoridade legal, mas também das capacidades produtivas que permitem às sociedades moldar as tecnologias pelas quais os dados são gerados, processados e trocados. Embora a soberania dos dados seja frequentemente discutida em termos de jurisdição, competência regulatória ou controle sobre fluxos de informação, essas dimensões legais e institucionais não podem ser plenamente realizadas na ausência de capacidades domésticas para desenvolver, adaptar, manter e governar infraestruturas digitais.⁸¹ A soberania, portanto, exige mais do que a autoridade para regular a mudança tecnológica; exige a capacidade de participar de forma significativa em sua produção e direção.

Essa compreensão reflete uma evolução mais ampla na própria política industrial. A política industrial contemporânea não foca mais principalmente na proteção das indústrias domésticas ou na correção de falhas isoladas do mercado. Em vez disso, busca cada vez mais moldar trajetórias tecnológicas coordenando investimentos públicos e privados em torno de missões estrategicamente definidas.⁸² Da mesma forma, Rodrik enfatiza que a política industrial moderna deve ser entendida como um processo de descoberta institucional pelo qual Estados e empresas desenvolvem conjuntamente capacidades produtivas sob condições de transformação⁸³ estrutural. Sob essa perspectiva, a política industrial não é simplesmente um instrumento para promover o crescimento econômico, mas um mecanismo pelo qual os governos expandem a capacidade de governança necessária para perseguir objetivos públicos coletivamente determinados.

Aplicada à economia digital, essa mudança tem implicações profundas. A capacidade produtiva não é mais medida principalmente pela capacidade de fabricação ou pela propriedade de ativos físicos. Em vez disso, depende cada vez mais da capacidade de projetar, implantar e melhorar continuamente sistemas sociotécnicos complexos, incluindo infraestruturas em nuvem, cadeias avançadas de suprimentos

⁸¹ Belli L. and others, *Soberania Digital e Inteligência Artificial no Brasil: Rumo à autonomia tecnológica* (Lumen-Juris 2026).

⁸² Mazzucato, Mariana. *The Entrepreneurial State: Debunking Public vs. Private Sector Myths*. London: Anthem Press, 2013. Revised edition, PublicAffairs, 2015.

⁸³ Rodrik, Dani. "Industrial Policy for the Twenty-First Century." Working paper prepared for UNIDO, September 2004.

de semicondutores, capacidades de cibersegurança, sistemas de IA e DPIs.⁸⁴ A soberania, portanto, depende menos da autossuficiência tecnológica do que da capacidade institucional de moldar a evolução desses sistemas tecnológicos interconectados.

Essa distinção é especialmente importante porque a transformação digital ocorre por meio de paradigmas tecnológicos sucessivos, e não de inovações isoladas. De fato, a capacidade de sustentar o desenvolvimento depende não apenas da invenção de novas tecnologias, mas de sua ampla difusão por sistemas e instituições produtivas⁸⁵. Países que desenvolvem com sucesso arranjos de governança capazes de absorver e adaptar mudanças tecnológicas frequentemente obtêm benefícios de longo prazo maiores do que aqueles que simplesmente geram inovações de fronteira. Do ponto de vista da soberania dos dados, isso implica que a capacidade de governança depende tanto da criação de novas tecnologias quanto de incorporá-las em estruturas institucionais, regulatórias e econômicas resilientes.

A própria inovação também se tornou cada vez mais ecossistêmica.⁸⁶ Em vez de ocorrer dentro de empresas isoladas, a inovação agora surge das interações entre desenvolvedores de tecnologia, provedores de infraestrutura, instituições públicas, organizações de pesquisa e prestadores de serviços complementares. Gawer mostrou que as plataformas digitais funcionam cada vez mais como ecossistemas de inovação cuja governança molda as oportunidades disponíveis para os participantes em toda a economia em geral⁸⁷. Essa observação amplia significativamente o significado da política industrial. A intervenção pública não se limita mais ao apoio a empresas ou setores individuais; Ela se preocupa cada vez mais com a governança dos ecossistemas pelos quais a inovação é gerada, coordenada e difundida.

Vista sob essa ótica, a política industrial contribui para a soberania dos dados ao fortalecer o que este artigo conceitua como capacidade de governança. Investimentos em pesquisa e desenvolvimento, habilidades digitais avançadas, cibersegurança, infraestrutura computacional confiável, padrões tecnológicos

⁸⁴ Belli, L. and Bhinder, A. Cooperative Digital Sovereignty and Artificial Intelligence Promoting Resilience, Strategic Openness, and Self-Determination. (Digital Cooperation Organization, 2026).

⁸⁵ Perez, Carlota. Technological Revolutions and Financial Capital: The Dynamics of Bubbles and Golden Ages. Cheltenham: Edward Elgar, 2002.

⁸⁶ Nicolo Zingales and Paula Farani de Azevedo (eds), *A Aplicação do Direito Antitruste em Ecossistemas Digitais: Desafios e Propostas* (FGV Direito Rio 2022)

⁸⁷ Gawer, Annabelle. "Digital Platforms' Boundaries: The Interplay of Firm Scope, Platform Sides, and Digital Interfaces." *Long Range Planning* 54, no. 5 (2021): 102045. See also Gawer, Annabelle. "Bridging Differing Perspectives on Technological Platforms: Toward an Integrative Framework." *Research Policy* 43, no. 7 (2014): 1239-1249.

abertos e infraestruturas públicas interoperáveis ampliam a gama de opções institucionais disponíveis para governos, empresas e sociedade civil. A soberania, portanto, torna-se menos uma questão de propriedade sobre ativos digitais e mais de preservar a capacidade coletiva de moldar o desenvolvimento tecnológico de acordo com prioridades democraticamente determinadas.⁸⁸

Essa perspectiva também ajuda a explicar por que a IA se tornou uma preocupação central da política industrial contemporânea. A capacidade de IA não deve ser equiparada apenas à capacidade de desenvolver modelos de fundação inovadores. Na verdade, a participação significativa na emergente economia de IA depende cada vez mais da capacidade de acessar e mobilizar Habilitadores Chave de Soberania em IA, como infraestrutura computacional, capacidade de avaliação, conjuntos de dados confiáveis, habilidades digitais avançadas e a capacidade institucional de implantar sistemas de IA de forma responsável em múltiplos setores.⁸⁹

A produção digital ocorre cada vez mais dentro de ecossistemas cuja operação não pode ser reduzida nem à coordenação descentralizada do mercado nem à direção hierárquica do estado. Os ecossistemas organizam complementaridades entre provedores de infraestrutura, desenvolvedores de aplicações, detentores de dados, instituições públicas e usuários, enquanto seus atores reguladores determinam as condições de acesso, interoperabilidade e criação de valor. Colaborativos de dados, por exemplo, devem ser tratados simplesmente como mecanismos para liberar conjuntos de dados adicionais. Sua importância reside na capacidade de estruturar a cooperação entre atores que possuem diferentes recursos, mandatos e responsabilidades, sujeitos a regras que regem acesso, propósito, responsabilidade e a alocação de benefícios e⁹⁰ riscos. Nesse sentido, eles ilustram como a capacidade produtiva pode ser sustentada por arranjos institucionais que não são exclusivamente dirigidos pelo Estado nem puramente proprietários.

Esses arranjos também revelam por que a política industrial digital deve ser entendida em termos policêntricos, e não exclusivamente centralizados. A explicação de Ostrom sobre governança policêntrica enfatiza que problemas coletivos complexos podem ser enfrentados por meio de múltiplos centros de tomada de decisão parcialmente autônomos, operando sob regras e mecanismos de

⁸⁸ Belli, L. and Bhinder, A. Cooperative Digital Sovereignty and Artificial Intelligence Promoting Resilience, Strategic Openness, and Self-Determination. (Digital Cooperation Organization, 2026).

⁸⁹ Belli, L. "To Get Its AI Foothold, Brazil Needs to Apply the Key AI Sovereignty Enablers (KASE)." In Feldstein S. (ed.) New Digital Dilemmas: Resisting Autocrats, Navigating Geopolitics, Confronting Platforms,. (Carnegie Endowment for International Peace, 2023) ; Belli L. and others, Soberania Digital e Inteligência Artificial no Brasil: Rumo à autonomia tecnológica (Lumen-Juris 2026).

⁹⁰ Zingales, Nicolo. "Data Collaboratives, Competition Law and the Governance of EU Data Spaces." In Research Handbook on the Law and Economics of Competition Enforcement, edited by Ioannis Kokkoris. Cheltenham: Edward Elgar, 202

coordenação sobrepostos.⁹¹ Aplicado ao desenvolvimento digital, isso sugere que a capacidade produtiva não precisa estar concentrada em um único ministério, empresa pública ou empresa nacionalmente favorecida. Pode, em vez disso, surgir da atividade coordenada de instituições de pesquisa, autoridades públicas, operadores de infraestrutura, empresas privadas, comunidades de código aberto e organizações da sociedade civil. A capacidade soberana relevante está em manter as condições institucionais sob as quais esses atores podem cooperar, experimentar e permanecer mutuamente responsáveis, enquanto impedem que qualquer centro de poder se torne estruturalmente indispensável.

Ao mesmo tempo, a política industrial precisa ser vista como um complemento essencial da política de concorrência: enquanto a primeira aumenta principalmente a autonomia tecnológica ao expandir as capacidades domésticas, a segunda aumenta principalmente a resiliência ao evitar dependência excessiva de empresas, tecnologias ou infraestruturas individuais.

Em última análise, a soberania dos dados exige ir além de uma concepção regulatória de governança em direção a uma concepção produtiva. Os Estados devem regular as tecnologias digitais, mas também devem possuir a capacidade de produzi-las, adaptá-las e melhorá-las continuamente. Governança e capacidade produtiva tornam-se dimensões mutuamente reforçadoras da soberania. No entanto, a capacidade produtiva sozinha não pode garantir soberania. Se a política industrial apenas substituir a concentração estrangeira pela concentração doméstica, a dependência tecnológica pode simplesmente mudar sua origem. Os benefícios do desenvolvimento industrial dependem, portanto, de estruturas de mercado competitivas capazes de preservar a contestabilidade, a inovação e a pluralidade tecnológica.

3.5. COMPETIÇÃO E INOVAÇÃO

Se a política industrial expande a gama de opções tecnológicas e produtivas disponíveis para uma sociedade, a política de concorrência ajuda a preservar essas opções ao evitar que o controle sobre os ecossistemas digitais se torne irreversivelmente concentrado. Portanto, as duas dimensões são complementares. Política industrial sem política de concorrência pode criar capacidades enquanto permite sua apropriação por um número limitado de empresas. A política de concorrência sem política industrial pode preservar a abertura formal do mercado enquanto não consegue gerar as infraestruturas, habilidades e organizações necessárias para uma participação significativa. A soberania dos dados exige ambos:

⁹¹ Ostrom, Elinor. "Polycentric Systems for Coping with Collective Action and Global Environmental Change." *Global Environmental Change* 20, no. 4 (2010): 550-557

a capacidade de desenvolver alternativas tecnológicas e arranjos institucionais que mantenham essas alternativas viáveis.

A relevância da política de concorrência para a soberania dos dados não pode ser totalmente captada pelas preocupações convencionais com preços, produção ou bem-estar do consumidor de curto prazo. Os mercados digitais são frequentemente caracterizados por efeitos de rede, economias de escala e escopo, acesso a grandes volumes de dados, altos custos de comutação e complementaridades entre serviços.⁹² Essas características podem permitir que uma empresa que controla uma camada estratégica de um ecossistema influencie a entrada e inovação em várias camadas adjacentes. O poder resultante não é apenas econômico. Inclui a capacidade de determinar interfaces técnicas, condições de acesso, padrão, práticas de compartilhamento de dados, regras de desenvolvedores e padrões de interoperabilidade. A concentração pode, portanto, transferir decisões que moldam a futura organização dos mercados digitais de instituições públicas e participantes dispersos do mercado para infraestruturas governadas privadamente.

Ecossistemas digitais tornam esse problema particularmente visível.⁹³ Eles consistem não apenas em coleções de produtos relacionados, mas em serviços, tecnologias e atores interdependentes organizados em torno de infraestruturas comuns e governados por interfaces, padrões e regras contratuais. Consequentemente, a competição ocorre tanto dentro dos ecossistemas quanto entre eles. Uma plataforma pode enfrentar competição em uma camada, mantendo influência decisiva sobre a infraestrutura ou portal da qual os concorrentes de outra camada dependem⁹⁴

Essa perspectiva ecossistêmica também exige uma compreensão mais precisa da inovação. A inovação não ocorre apenas por meio da rivalidade entre empresas verticalmente integradas que produzem produtos substituíveis. Frequentemente depende de complementaridades entre provedores de infraestrutura, desenvolvedores de aplicações, detentores de dados e usuários. Decisões de governança sobre acesso a interfaces, portabilidade, interoperabilidade e dados podem, portanto, determinar quem pode inovar, em quais termos e em qual camada tecnológica. O objetivo relevante não é maximizar o número de concorrentes em

⁹² Nicolo Zingales and Paula Farani de Azevedo (eds), *A Aplicação do Direito Antitruste em Ecossistemas Digitais: Desafios e Propostas* (FGV Direito Rio 2022)

⁹³ Idem.

⁹⁴ Veja, por exemplo, Jacobides, Michael G., and Ioannis Lianos. "Ecosystems and Competition Law in Theory and Practice." *Industrial and Corporate Change* 30, no. 5 (2021): 1199–1229.; Zingales, Nicolo, and Bruno Polonio Renzetti. "Digital Platform Ecosystems and Conglomerate Mergers: A Review of the Brazilian Experience." *World Competition* 45, no. 4 (2022): 473–514.

abstrato, mas preservar um ambiente institucional no qual serviços alternativos, modelos de negócios e trajetórias tecnológicas possam surgir.

A política de concorrência contribui para a soberania ao preservar essa opcionalidade de governança. A contestabilidade garante que governos, empresas e usuários não fiquem permanentemente confinados aos padrões, arranjos contratuais ou direção tecnológica escolhidos por uma empresa dominante. A possibilidade de trocar de fornecedor, combinar serviços, acessar interfaces essenciais ou desenvolver alternativas interoperáveis preserva a capacidade de atores públicos e privados de revisar as escolhas tecnológicas ao longo do tempo. Nesse sentido, a competição protege não apenas a rivalidade presente, mas também a escolha institucional futura.

Essa afirmação não implica que toda forma de concentração seja incompatível com a inovação. Economias de escala significativas podem ser necessárias para computação em nuvem, fabricação de semicondutores, infraestrutura de pagamentos e inteligência artificial de vanguarda. Grandes empresas podem possuir recursos que possibilitam formas caras e arriscadas de pesquisa e desenvolvimento. A preocupação com a soberania surge quando a escala se torna estruturalmente indispensável: quando governos, empresas ou usuários não podem realisticamente migrar, interoperar ou apoiar alternativas sem custos ou interrupções proibitivas.⁹⁵ A política de concorrência, portanto, deveria focar não apenas no tamanho das empresas, mas também em saber se a governança do ecossistema preserva viáveis caminhos de saída, entrada, substituição e inovação.

Conduta relacionada a dados oferece um exemplo particularmente importante. Os dados podem ser usados para melhorar produtos e coordenar serviços, mas também podem ser usados para excluir rivais, explorar usuários dependentes, discriminar parceiros de negócios ou estender poder para atividades adjacentes. A importância jurídica de uma prática depende da posição ocupada pela empresa, da função dos dados dentro do ecossistema relevante, da relação entre as partes e dos efeitos excludentes ou exploratórios produzidos. Essa abordagem diferenciada é compatível com o arcabouço desenvolvido aqui: a soberania dos dados é minada não pela concentração de dados em si, mas pelo uso de dados que bloqueiam alternativas institucionais, consolidam a dependência ou impedem os atores afetados de participar em termos justos.

Essas preocupações explicam o movimento crescente da aplicação exclusivamente ex post para formas mais explícitas de governança digital ex ante do mercado. O

⁹⁵ Belli L. and others, *Soberania Digital e Inteligência Artificial no Brasil: Rumo à autonomia tecnológica* (Lumen-Juris 2026).

relatório da Comissão Europeia, elaborado por Crémer, de Montjoye e Schweitzer⁹⁶, argumentou que as características da economia digital exigem a adaptação de conceitos, metodologias e soluções do direito da concorrência, especialmente em relação a plataformas, dados e inovação. A Revisão Furman⁹⁷ também propôs um regime regulatório pró-concorrência centrado em empresas com status estratégico de mercado, acompanhado de regras sobre interoperabilidade, mobilidade de dados e medidas de abertura de mercado. Essas iniciativas ajudaram a estabelecer as bases intelectuais para regimes contemporâneos, como a Lei dos Mercados Digitais da União Europeia e o marco dos mercados digitais do Reino Unido.

A importância dessa evolução regulatória não está apenas na introdução de obrigações adicionais para grandes empresas. Reflete uma mudança no objetivo da governança da competição. Em vez de intervir apenas após uma infração claramente definida dentro de um determinado mercado, a regulação digital busca cada vez mais manter as condições institucionais de contestabilidade entre os ecossistemas. Obrigações relacionadas à interoperabilidade, portabilidade, acesso a dados, autopreferência, vinculação e governança de lojas de aplicações ou sistemas operacionais são direcionadas à arquitetura pela qual ocorre a coordenação econômica. A lei e a regulamentação da concorrência tornam-se, assim, mecanismos para governar o poder infraestrutural.

A Infraestrutura Pública Digital pode reforçar esses objetivos, mas apenas sob condições específicas de governança. Ao transformar funções de identidade, pagamento ou troca de dados em capacidades compartilhadas e interoperáveis, o DPI pode reduzir a necessidade de cada participante do mercado reproduzir a infraestrutura fundamental. Infraestruturas modulares separam as camadas fundamentais das camadas de aplicação competitivas, facilitando a inovação distribuída enquanto reduzem o lock-in⁹⁸. Isso pode reduzir os custos de entrada e permitir a concorrência no nível das inscrições e serviços complementares. Pix e UPI ilustram como os trilhos de pagamento comuns podem permitir que bancos e empresas fintech inovem dentro de uma arquitetura compartilhada, em vez de competir por meio de redes proprietárias fechadas.

No entanto, o caráter público da infraestrutura não garante automaticamente resultados competitivos. O DPI pode, por si só, reforçar a concentração de mercado

⁹⁶ Crémer, Jacques, Yves-Alexandre de Montjoye and Heike Schweitzer. Competition Policy for the Digital Era. European Commission, 2019

⁹⁷ Digital Competition Expert Panel. Unlocking Digital Competition. HM Treasury, 2019, commonly referred to as the Furman Review

⁹⁸ Baldwin, Carliss Y., and Kim B. Clark. Design Rules, Volume 1: The Power of Modularity. MIT Press, 2000.

se as condições de acesso forem discriminatórias, os padrões técnicos forem controlados por incumbentes, as práticas de aquisição criarem dependência de fornecedores insubstituíveis ou a interoperabilidade for apenas nominal. Portanto, o DPI que potencializa a competição exige padrões abertos, interfaces documentadas, portabilidade, design modular, governança transparente e condições de acesso proporcionais que permitam participação significativa e substituição tecnológica.⁹⁹

A licitação pública constitui um instrumento fundamental nesse sentido. Como grandes compradores de serviços em nuvem, software, cibersegurança e inteligência artificial, os governos podem moldar a estrutura do mercado por meio de requisitos de interoperabilidade, auditoria, padrões abertos, portabilidade de dados e estratégias de saída, fortalecendo tanto a concorrência quanto a autonomia pública.

Da mesma forma, colaborativos de dados podem ampliar o acesso a conjuntos de dados valiosos e fomentar a inovação nos setores público, privado e de pesquisa, desde que operem sob arranjos claros de governança. Sua contribuição para ecossistemas digitais competitivos depende de regras transparentes de participação, acesso equitativo, salvaguardas adequadas e mecanismos de responsabilização que previnam o surgimento de novos gatekeepers.¹⁰⁰

Em última análise, a governança da concorrência em ecossistemas digitais exige uma abordagem policêntrica envolvendo autoridades de concorrência, reguladores de proteção de dados, agências de cibersegurança, órgãos de aquisição e organizações de padronização. Do ponto de vista da soberania dos dados, a política de concorrência desempenha três funções essenciais: prevenir a concentração do poder infraestrutural, preservar a pluralidade tecnológica por meio da interoperabilidade e substituição, e permitir que uma gama mais ampla de atores participe da inovação digital. A competição, portanto, não é apenas um objetivo econômico, mas uma condição constitucional para manter o controle coletivo sobre a transformação digital.

No entanto, ecossistemas competitivos não podem ser sustentados apenas por intervenção regulatória. Autoridades de concorrência, infraestruturas públicas, sistemas de pesquisa e políticas de inovação exigem recursos financeiros duradouros, enquanto o valor gerado nos ecossistemas digitais permanece distribuído de forma desigual. A preservação da opcionalidade da governança leva,

⁹⁹ Doctorow, C. (2021). *How to destroy surveillance capitalism*. Medium Editions.

¹⁰⁰ Zingales, Nicolò. "Data Collaboratives, Competition Law and the Governance of EU Data Spaces." In *Research Handbook on the Law and Economics of Competition Enforcement*, edited by Ioannis Kokkoris. Cheltenham: Edward Elgar, 2022.

portanto, diretamente à sexta dimensão da soberania dos dados: a capacidade fiscal de manter esses arranjos institucionais e garantir que a atividade econômica orientada por dados contribua para um valor público mais amplo. A competição preserva não apenas a rivalidade atual, mas também as oportunidades futuras de inovação ao evitar o bloqueio tecnológico irreversível¹⁰¹.

3.6. JUSTIÇA FISCAL E EQUIDADE DE DADOS

Talvez a dimensão menos explorada da soberania dos dados diga respeito à tributação. No entanto, a capacidade fiscal historicamente constituiu um dos atributos definidores da autoridade soberana. Desde o surgimento do Estado moderno, a capacidade de arrecadar receita permitiu aos governos fornecerem bens públicos, manter instituições, investir em infraestrutura e buscar objetivos de desenvolvimento. A transformação digital não diminuiu a importância da tributação; na verdade, alterou fundamentalmente as condições sob as quais o valor é criado e distribuído.

Modelos de negócios intensivos em dados geram um valor econômico extraordinário por meio de atividades que frequentemente transcendem os conceitos tradicionais de presença física ou estabelecimento territorial. Plataformas digitais podem obter receitas substanciais de usuários localizados em uma jurisdição, mantendo uma presença tributável limitada sob as regras fiscais internacionais convencionais. Da mesma forma, dados gerados coletivamente pelas sociedades contribuem significativamente para o desenvolvimento de sistemas de IA, publicidade direcionada, otimização algorítmica e inúmeras outras aplicações comercialmente valiosas cujos retornos econômicos permanecem altamente concentrados.

Esses desenvolvimentos levantam questões que vão além da administração tributária. Eles tratam da distribuição do valor gerado pela própria economia digital.¹⁰² Se os dados forem cada vez mais reconhecidos como recursos econômicos estratégicos, então os benefícios derivados de sua exploração deveriam contribuir para um bem-estar social mais amplo, em vez de se apropriar exclusivamente daqueles que possuem maior capacidade tecnológica ou poder de mercado. A política fiscal, portanto, torna-se um instrumento pelo qual as sociedades podem

¹⁰¹ Federico, Giulio, Fiona Scott Morton and Carl Shapiro. "Antitrust and Innovation: Welcoming and Protecting Disruption." *Innovation Policy and the Economy* 20 (2020): 125–190. (Originally NBER Working Paper No. 26005, 2019.)

¹⁰² Belli L., Fossati G. McClaskey L. and Zingales, N. *Proteção, Tributação e Equidade de Dados: Equilibrando Valores, Riscos e Obrigações na Economia Digital*. (Lumen Juris 2026)

garantir que a transformação digital apoie o desenvolvimento inclusivo, em vez de reforçar desigualdades existentes.

Iniciativas internacionais recentes lideradas pelo Quadro Inclusivo OCDE/G20 buscaram adaptar a tributação internacional aos desafios impostos por modelos de negócios altamente digitalizados.¹⁰³ Embora essas reformas representem progressos importantes, elas abordam principalmente questões relacionadas à alocação de direitos tributários e à tributação mínima das empresas. A relação mais ampla entre tributação e governança de dados continua relativamente subdesenvolvida.

Portanto, esta seção propõe compreender a tributação como uma dimensão integral da soberania dos dados, em vez de uma área separada da política fiscal. Primeiro, a tributação fornece aos governos os recursos necessários para investir em cibersegurança, infraestrutura pública digital, educação digital, pesquisa e inovação. Sem capacidade fiscal adequada, muitas das outras dimensões da soberania tornam-se difíceis de sustentar ao longo do tempo.

Segundo, a tributação contribui para corrigir assimetrias distributivas geradas por mercados digitais altamente concentrados. O investimento público financiado por receitas geradas pela atividade econômica digital pode apoiar uma participação mais ampla na transformação digital, fortalecendo assim tanto a coesão social quanto a resiliência econômica.

Terceiro, a política fiscal pode incentivar uma governança responsável dos dados por meio de incentivos adequadamente elaborados. Medidas fiscais que apoiam investimentos em cibersegurança, infraestruturas digitais confiáveis, tecnologias abertas ou ecossistemas de inovação doméstica ilustram como instrumentos fiscais podem reforçar objetivos de governança mais amplos.

Por fim, a tributação deve ser entendida dentro do conceito mais amplo de equidade de dados.¹⁰⁴ Os dados raramente são criados por indivíduos isolados agindo de forma independente. Elas surgem por meio de interações complexas envolvendo cidadãos, empresas, instituições públicas e infraestruturas digitais. Seu valor econômico, portanto, é inerentemente relacional e coletivo. Pela equidade de dados reconhece-se que as sociedades que contribuem para a criação desse valor possuem reivindicações legítimas sobre sua distribuição e uso público.

Isso não implica a cessão de direitos de propriedade proprietária sobre todos os dados gerados dentro de uma jurisdição. Em vez disso, indica que os governos têm

¹⁰³ Organisation for Economic Co-operation and Development (OECD), *Addressing the Tax Challenges of the Digital Economy, Action 1 – 2015 Final Report* (OECD/G20 Base Erosion and Profit Shifting Project, OECD Publishing 2015) ; OECD, *Tax Challenges Arising from Digitalisation – Report on Pillar One Blueprint: Inclusive Framework on BEPS* (OECD/G20 Base Erosion and Profit Shifting Project, OECD Publishing 2020)

¹⁰⁴ Belli L., Fossati G. McClaskey L. and Zingales, N. Proteção, Tributação e Equidade de Dados: Equilibrando Valores, Riscos e Obrigações na Economia Digital. (Lumen Juris 2026)

autoridade legítima para projetar estruturas fiscais e regulatórias que garantam que a transformação digital contribua para o desenvolvimento econômico inclusivo, investimento social e bem-estar público. Assim, a justiça fiscal constitui uma dimensão constitutiva essencial da soberania dos dados, considerando que, sem recursos públicos sustentáveis, as capacidades institucionais necessárias para uma soberania significativa não podem ser mantidas. Assim como a tributação historicamente possibilitou a construção de estradas, escolas, tribunais e sistemas de saúde pública, ela financia cada vez mais as infraestruturas digitais das quais depende a soberania contemporânea.

3.7. SOBERANIA DE DADOS COMO FRAMEWORK INTEGRADA DE GOVERNANÇA

A análise anterior mostra que a soberania dos dados não pode ser reduzida a uma única doutrina jurídica, ativo tecnológico ou instrumento de política. A soberania dos dados é melhor compreendida como uma capacidade institucional emergente produzida pela interação de arranjos legais, tecnológicos, econômicos e administrativos mutuamente reforçados.

As seis dimensões examinadas nesta seção desempenham cada uma função de governança distinta. A proteção de dados fornece a base de legitimidade baseada em direitos, ao salvaguardar a autodeterminação informativa e as liberdades fundamentais. A cibersegurança protege a integridade, disponibilidade e resiliência dos sistemas digitais dos quais a autoridade pública depende cada vez mais. A Infraestrutura Pública Digital oferece capacidades institucionais compartilhadas pelas quais direitos, serviços e funções públicas podem ser operacionalizados em larga escala. O desenvolvimento industrial e a capacidade tecnológica sustentam a base produtiva necessária para projetar, manter e adaptar infraestruturas digitais estratégicas. A concorrência e a inovação preservam a abertura, a contestabilidade e a pluralidade tecnológica. Justiça fiscal e equidade em dados fornecem os recursos e mecanismos distributivos necessários para garantir que a transformação digital gere valor público, e não apenas acúmulo privado.

Um mecanismo de governança voltado para construir soberania dos dados deve atuar como camada coordenadora entre essas dimensões, e não como uma dimensão constitutiva adicional. Ela atribui autoridade, responsabilidade, acesso, responsabilidade e reparação em relação aos dados e seus usos legítimos. Ao fazer isso, conecta direitos, infraestrutura, segurança, mercados, política industrial e capacidade fiscal dentro de uma arquitetura institucional coerente. Sem essa coordenação, as seis dimensões correm o risco de permanecer fragmentadas: a proteção de dados pode estabelecer direitos formais sem uma aplicação eficaz; a cibersegurança pode proteger sistemas sem responsabilidade democrática; O DPI pode possibilitar a prestação de serviços sem salvaguardas adequadas; a política

industrial pode construir capacidade sem inclusão; a política de concorrência pode abrir mercados sem garantir o valor público; e a política fiscal pode aumentar a receita sem fortalecer as bases institucionais da soberania.

Essa concepção integrada fornece o retorno analítico do arcabouço. Isso explica por que abordagens parciais à governança digital frequentemente não produzem soberania significativa. Portanto, a soberania dos dados não está localizada em um conjunto de dados, servidores, plataformas, estatutos ou órgãos públicos. Ela é produzida por meio das relações entre instituições, infraestruturas, regras e capacidades que permitem as autoridades democráticas governarem a transformação digital de forma legítima, eficaz e responsável. Isso também significa que a soberania é dinâmica, e não estática, e, portanto, qualquer governança orientada para a soberania precisa ser sustentada por mecanismos sólidos de consciência situacional, capazes de identificar ameaças, avaliar riscos e apoiar decisões informadas e oportunas.¹⁰⁵ Ela deve ser mantida continuamente à medida que tecnologias, mercados, riscos e condições geopolíticas evoluem. Uma arquitetura de governança que é soberana em determinado momento pode se tornar dependente ou frágil se não conseguir se adaptar a novos padrões tecnológicos, ameaças à segurança, estruturas de mercado ou formas de extração de valor.

Essa perspectiva também esclarece por que os debates sobre soberania de dados frequentemente parecem fragmentados ou contraditórios. Diferentes comunidades epistêmicas enfatizam diferentes partes do mesmo problema institucional. Constitucionalistas focam em direitos, dignidade e autonomia. Especialistas em cibersegurança priorizam a resiliência e a proteção de infraestruturas críticas. Profissionais da administração pública enfatizam a capacidade estadual e a prestação de serviços. Economistas examinam inovação, concentração e distribuição de valor. Pesquisadores preocupados com o desenvolvimento socioeconômico destacam dependência, desigualdade e capacidade tecnológica. Cada perspectiva identifica um componente real da soberania, mas nenhuma sozinha captura o desafio completo da governança.

Compreender a soberania dos dados como um arcabouço integrado de governança permite articular essas diferentes perspectivas em torno de um projeto institucional comum. Seu objetivo central é preservar a capacidade de indivíduos, sociedades e Estados de moldar as condições jurídicas, técnicas e econômicas sob as quais dados e infraestruturas digitais são governados. O exercício dessa capacidade pressupõe a articulação entre direitos e segurança dos sistemas, infraestrutura pública e capacidade produtiva, funcionamento dos mercados, contestabilidade e distribuição

¹⁰⁵ Belli L. and others, Soberania Digital e Inteligência Artificial no Brasil: Rumo à autonomia tecnológica (Lumen-Juris 2026).

equitativa de seus benefícios, bem como autoridade interna e mecanismos institucionais aptos a administrar as interdependências transnacionais.

Esse ponto final fornece a transição para a próxima seção. Se a soberania dos dados é uma capacidade integrada e não apenas controle territorial sobre os dados, a questão decisiva passa a ser como essa capacidade pode ser exercida dentro de ecossistemas digitais que são inerentemente transnacionais. A resposta não pode ser o isolamento tecnológico. Deve estar em formas de cooperação que preservem a agência enquanto possibilitam a interdependência. Portanto, a Seção 4 examina como a governança digital soberana pode ser perseguida por meio de instituições interoperáveis, Infraestrutura Pública Digital compartilhada e cooperação internacional fundamentada na reciprocidade, resiliência e igualdade soberana dos Estados.

4. COMO CONSTRUIR SOBERANIA DE DADOS

A seção anterior argumentou que a soberania dos dados deve ser melhor entendida como uma capacidade integrada de governança, e não como controle territorial sobre dados ou autossuficiência tecnológica. Ela surge da interação de seis dimensões mutuamente reforçadoras: proteção de dados, cibersegurança e resiliência digital, Infraestrutura Pública Digital, desenvolvimento industrial e capacidade tecnológica, competição e inovação, e justiça fiscal e equidade de dados. A governança orientada à soberania de dados coordena essas dimensões ao alocar autoridade, responsabilidade, acesso, prestação de contas e reparação em toda a arquitetura institucional pela qual a transformação digital é governada.

A questão que segue é de como essa capacidade integrada pode ser exercida dentro de ecossistemas digitais que são inerentemente transnacionais. Isto está no centro dos debates contemporâneos sobre soberania digital. Como enfatizamos, grande parte da discussão tem sido enquadrada em torno da autossuficiência tecnológica, localização de dados e controle doméstico sobre ativos digitais críticos. Essas preocupações respondem a riscos geopolíticos, econômicos e de segurança reais, especialmente quando os Estados dependem de infraestruturas, padrões ou fornecedores sobre os quais têm pouca influência. No entanto, também correm o risco de apresentar a soberania como uma condição que pode ser alcançada principalmente por meio do controle territorial ou do isolacionismo tecnológico.

Tal compreensão pode ser incorreta e cada vez mais difícil de conciliar com a arquitetura do ambiente digital contemporâneo, onde concentração e distribuição coexistem. Os dados rotineiramente atravessam múltiplas jurisdições em frações de segundo. As infraestruturas de nuvem são geograficamente distribuídas. Modelos de IA são desenvolvidos por meio de comunidades de pesquisa dispersas globalmente e treinados com conjuntos de dados de origem internacional. Softwares de código aberto sustentam grande parte da infraestrutura digital atual, enquanto o

comércio digital depende de padrões técnicos interoperáveis, credenciais confiáveis e estruturas regulatórias compatíveis. Portanto, a autonomia tecnológica completa não é nem alcançável na prática nem institucionalmente desejável.

O desafio que os Estados enfrentam, portanto, não é como eliminar a interdependência, mas como governá-la. A soberania é enfraquecida não pela adoção de tecnologias estrangeiras, mas por formas de dependência que privam as instituições públicas de uma agência significativa sobre as condições legais, institucionais e tecnológicas pelas quais a autoridade pública é exercida.¹⁰⁶

Portanto, esta seção redefine a soberania dos dados como capacidade de governança cooperativa. A soberania não consiste em impedir que dados, serviços ou infraestruturas cruzem fronteiras, mas em preservar a capacidade das instituições democráticas de determinar as condições sob as quais dados, autoridade pública e confiança institucional podem legitimamente circular entre elas.

4.1. IGUALDADE SOBERANA COMO FUNDAÇÃO

Se a seção anterior estabeleceu a soberania dos dados como uma capacidade institucional integrada, a subseção atual questiona como essa capacidade pode ser exercida entre atores formalmente iguais, mas materialmente desiguais. A resposta começa com o princípio da igualdade soberana. No ambiente digital, entretanto, a igualdade soberana não pode ser entendida apenas como status jurídico igualitário. Também deve ser entendida em termos da agência institucional necessária para exercer autoridade pública de forma eficaz dentro dos ecossistemas digitais transnacionais.

O Artigo 2(1) da Carta das Nações Unidas estabelece a igualdade soberana de todos os Estados-Membros, afirmando que os Estados gozam de status jurídico igual, independentemente das diferenças de território, população, poder econômico ou influência geopolítica. Tradicionalmente, esse princípio tem governado as relações diplomáticas, a elaboração de tratados, a competência jurisdicional e a resolução pacífica de disputas. Ela fornece a base normativa sobre a qual comunidades políticas independentes cooperam sem renunciar a sua autonomia jurídica e institucional.

¹⁰⁶ Belli L. and others, *Soberania Digital e Inteligência Artificial no Brasil: Rumo à autonomia tecnológica* (Lumen-Juris 2026); Belli, L. and Bhinder, A. *Cooperative Digital Sovereignty and Artificial Intelligence Promoting Resilience, Strategic Openness, and Self-Determination*. (Digital Cooperation Organization, 2026).

A transformação digital revela os limites dessa compreensão formal. A igualdade jurídica entre os Estados não necessariamente se traduz em igual capacidade de influenciar as infraestruturas, os padrões e os sistemas tecnológicos que estruturam o ambiente digital e, cada vez mais, condicionam a distribuição e o exercício do poder.

A igualdade soberana no ecossistema digital deve, portanto, ser entendida não apenas como igualdade jurídica, mas como agência institucional: a capacidade das instituições públicas de compreender, moldar, auditar, contestar e revisar as condições legais, organizacionais e tecnológicas sob as quais a autoridade pública é exercida. Essa compreensão estende, em vez de substituir, a doutrina tradicional da igualdade soberana. A soberania formal continua indispensável, mas torna-se insuficiente quando os governos não conseguem influenciar de forma significativa os padrões, infraestruturas, contratos ou capacidades tecnológicas dos quais dependem funções públicas essenciais.¹⁰⁷

Isso não exige que todos os estados possuam capacidades tecnológicas idênticas. Tal padrão seria irrealista e normativamente desnecessário. A igualdade soberana exige, em vez disso, que a participação em ecossistemas digitais não seja estruturada de forma a tornar alguns Estados permanentemente dependentes de infraestruturas, padrões, fornecedores ou arranjos de governança que eles não possam auditar, influenciar ou substituir de forma significativa. A interdependência é compatível com a soberania quando preserva escolha, reciprocidade e adaptabilidade institucional. A dependência surge quando relações assimétricas permitem que um ator restrinja as legítimas escolhas públicas de outro.

Notavelmente, essas assimetrias não se limitam mais às relações entre Estados. Os ecossistemas digitais contemporâneos também são caracterizados por concentrações sem precedentes de poder infraestrutural dentro de um número relativamente pequeno de atores privados. Provedores de nuvem, plataformas digitais, redes de pagamento, mercados de aplicações, fornecedores de soluções de cibersegurança e desenvolvedores de modelos fundamentais de IA operam cada vez mais infraestruturas cuja importância vai além da atividade comercial comum. Seus sistemas podem se tornar funcionalmente públicos quando mediam acesso a serviços públicos, transações financeiras, verificação de identidade, comunicação administrativa ou atualizações de segurança. Decisões sobre interoperabilidade, precificação, arquiteturas de segurança, portabilidade de dados, condições de acesso ou continuidade do serviço podem, portanto, moldar as condições operacionais sob as quais a autoridade pública é exercida, mesmo sem qualquer violação formal do direito internacional.

¹⁰⁷ Idem.

Aplicar igualdade soberana à governança digital, consequentemente, exige mais do que respeito à jurisdição territorial ou ao princípio da não intervenção. Exige garantir que os Estados possuam oportunidades significativas para participar da formação das infraestruturas, padrões, estruturas de governança e arranjos institucionais que organizam a economia digital global. Essa consideração é particularmente importante para países em desenvolvimento, que frequentemente contribuem com dados, usuários, inovação e valor social para os ecossistemas digitais globais, enquanto capturam apenas uma parcela limitada dos benefícios tecnológicos, institucionais e econômicos resultantes.¹⁰⁸

A soberania dos dados adquire, consequentemente, uma dimensão internacional essencial. Ela diz respeito não apenas à autoridade interna dos Estados para regular dados, mas também à sua capacidade de participar de forma horizontal, como pares institucionais, na formação das condições legais, técnicas e organizacionais pelas quais os ecossistemas digitais evoluem. A soberania, portanto, é fortalecida não por meio do isolamento tecnológico, mas por meio de arranjos institucionais que preservam a autonomia enquanto possibilitam cooperação sob condições de reciprocidade, resiliência e confiança mútua. Autonomia significativa depende menos da eliminação da interdependência do que de preservar a capacidade de fazer, contestar e revisar escolhas tecnológicas ao longo do tempo.

Esse princípio normativo, no entanto, não pode operar apenas por reconhecimento jurídico. A igualdade soberana sustenta a afirmação de que instituições e jurisdições devem cooperar de modo equânime. A interoperabilidade fornece os meios operacionais para que essa reivindicação adquira concretude administrativa, jurídica e técnica. Ela permite que instituições e jurisdições autônomas troquem informações, reconheçam credenciais, coordenem serviços públicos e estabeleçam interações confiáveis com base em padrões compartilhados e arranjos comuns de governança, preservando sua autonomia institucional e dispensando estruturas hierárquicas de controle. A interoperabilidade, portanto, contribui para definir a igualdade soberana, fundamento do direito internacional, em capacidade efetiva de atuação na governança digital, estabelecendo uma conexão institucional entre autonomia, interdependência e cooperação.

¹⁰⁸ Avila Pinto, R. (2018). Digital sovereignty or digital colonialism? New tensions of privacy, security and national policies. *SUR: International Journal on Human Rights*, 15(27), 15–27; Couldry, N., & Mejias, U. A. (2019). *The costs of connection: How data is colonizing human life and appropriating it for capitalism*. Stanford University Press; Benyera, E. *The Fourth Industrial Revolution and the Recolonisation of Africa: The Coloniality of Data*. (Routledge, 2021);

4.2. INTEROPERABILIDADE COMO EXPRESSÃO OPERACIONAL DA SOBERANIA

Se a igualdade soberana oferece a base normativa para a cooperação em ambientes digitais, a interoperabilidade fornece uma das respostas operacionais pela qual essa igualdade pode ser exercida. A igualdade soberana não é autoexecutável em sistemas digitais. Exige arranjos concretos pelos quais Estados, instituições públicas e outros atores juridicamente autônomos possam cooperar sem hierarquia, dependência ou perda de responsabilidade constitucional. A interoperabilidade fornece um dos principais mecanismos pelos quais tal cooperação se torna possível. Não se trata apenas da capacidade técnica dos sistemas para trocar e usar dados, mas da capacidade de governança das instituições autônomas de interagir sob regras compartilhadas, preservando seus mandatos legais, responsabilidade democrática e autoridade de decisão.

Nesse sentido, a interoperabilidade dá expressão externa à concepção integrada de soberania dos dados desenvolvida na Seção III. Proteção de dados, cibersegurança, infraestrutura pública digital, capacidade industrial, concorrência e capacidade fiscal tornam-se mutuamente reforçadas apenas quando as instituições conseguem coordenar entre as fronteiras organizacionais e jurisdicionais sob condições legítimas e responsáveis. A interoperabilidade, portanto, não é uma dimensão adicional da soberania, mas a gramática operacional através da qual as diferentes dimensões da soberania podem interagir sem colapsar em uma única autoridade.¹⁰⁹

Esse entendimento exige ir além da interpretação convencional da interoperabilidade como uma capacidade puramente técnica.¹¹⁰ Como argumenta Lessig, a arquitetura funciona como uma forma de regulação ao moldar as condições sob as quais o comportamento se torna possível.¹¹¹ No entanto, a interoperabilidade

¹⁰⁹ Belli, L. and Zingales, N. (2023). "Interoperability to foster open digital ecosystems in the BRICS countries" (提升互操作性, 构建金砖国家开放数字生态系统). in Chinese Academy of Cyberspace Studies, Xinhua Institute, China Institute of International Studies (中国网络空间研究院·新华社研究院·中国国际问题研究院). Shared Vision for the Digital World: Insights from Global Think Tanks on Jointly Building a Community with a Shared Future in Cyberspace (数字世界的共同愿景: 全球智库论携手构建网络空间命运共同体). The Commercial Press (商务印书馆)

¹¹⁰ Ian Brown, *Interoperability as a Tool for Competition Regulation* (OpenForum Academy 2020)

¹¹¹ Lessig, L. Code: Version 2.0 (Basic Books 2006); Mireille Hildebrandt, 'Algorithmic Regulation and the Rule of Law' (2018) 376(2128) *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 20170355

dentro da governança pública vai além da regulamentação por meio de arquitetura técnico. Ela faz parte da arquitetura institucional pela qual a autoridade pública é exercida, coordenada e limitada através das fronteiras organizacionais. Ela permite que princípios constitucionais e administrativos sejam traduzidos em práticas, procedimentos e sistemas tecnicamente operacionais, preservando os marcos jurídicos e institucionais que lhes conferem fundamento e legitimidade. Nesse sentido, a interoperabilidade deve ser compreendida como um mecanismo institucional e técnico de implementação de governança em ambientes digitais.¹¹²

A legitimidade dessa implementação depende do arcabouço de governança de dados dentro do qual ocorrem trocas interoperáveis. Decisões sobre quem detém autoridade sobre informações, os propósitos para os quais as informações podem ser processadas, a base legal que permite a troca e os mecanismos de responsabilidade e reparação aplicáveis a essas trocas não podem ser determinadas apenas pela compatibilidade técnica. Essas questões dizem respeito à alocação de autoridade pública, e não à movimentação de dados. A governança determina se uma interação é legítima; o objetivo da interoperabilidade deve ser determinar como essa interação legítima é implementada através das fronteiras institucionais.

Esse ponto está diretamente relacionado ao papel da proteção de dados identificado na Seção 3.1. A interoperabilidade deve visar facilitar a interação governada entre instituições autônomas, preservando legalidade, justiça, transparência, limitação de propósitos, proporcionalidade, minimização de dados, responsabilidade e reparação. A teoria da integridade contextual de Helen Nissenbaum¹¹³ oferece uma visão importante nesse sentido: a legitimidade dos fluxos de informação depende não apenas da conectividade técnica, mas da preservação das normas contextuais que regem as relações institucionais. Portanto, a interoperabilidade protege a soberania apenas quando sustenta, e não corrói, o contexto legal e institucional dentro do qual os dados são trocados.

A importância da interoperabilidade, portanto, vai além do próprio movimento de informação.¹¹⁴ Toda interação interoperável pressupõe uma relação de reconhecimento institucional. A interoperabilidade funciona como um mecanismo de governança pelo qual a confiança institucional é organizada e operacionalizada. Essa confiança deriva não exclusivamente da garantia criptográfica ou das

¹¹² Ian Brown, *Interoperability as a Tool for Competition Regulation* (OpenForum Academy 2020)

¹¹³ Helen Nissenbaum, 'Privacy as Contextual Integrity' (2004) 79(1) *Washington Law Review* 119–158

¹¹⁴ Ian Brown, *Interoperability as a Tool for Competition Regulation* (OpenForum Academy 2020)

comunicações seguras, mas dos mandatos legais, arranjos de governança e mecanismos de responsabilização que conferem legitimidade à ação institucional.

Essa compreensão institucional é consistente com a concepção de governança policêntrica de Ostrom¹¹⁵ e com a visão da soberania de dados como um arcabouço integrado de governança desenvolvido na Seção 3.7. Em vez de concentrar a autoridade em uma única plataforma tecnológica ou hierarquia administrativa, ecossistemas digitais interoperáveis distribuem a responsabilidade entre múltiplas instituições autônomas operando sob regras compartilhadas. Arranjos federados de governança permitem que fontes autoritativas permaneçam dentro das instituições legalmente responsáveis por produzi-las e mantê-las, ao mesmo tempo em que possibilitam cooperação legítima por meio de padrões comuns e interfaces confiáveis. A soberania, portanto, é preservada não por meio da centralização, mas pela autonomia institucional coordenada.

A interoperabilidade depende, conseqüentemente, de várias dimensões mutuamente reforçadas. A interoperabilidade normativa estabelece fundamentos conceituais suficientemente compatíveis para apoiar a cooperação. A interoperabilidade jurídica¹¹⁶ fornece regras compatíveis que regem autoridade, responsabilidade, reconhecimento e recursos. A interoperabilidade organizacional alinha mandatos institucionais, arranjos de governança e responsabilidades operacionais. A interoperabilidade semântica preserva o significado, a proveniência e a compreensibilidade da informação em contextos institucionais. A interoperabilidade técnica fornece os protocolos, interfaces, mecanismos de cibersegurança e serviços de confiança pelos quais as interações autorizadas se tornam operacionais. Juntas, essas dimensões mostram por que a interoperabilidade é melhor entendida como cooperação governada e não apenas conectividade.

Essas dimensões não devem ser entendidas como camadas independentes, mas como componentes complementares de uma única arquitetura de governança. Abbott e Snidal mostraram que a governança contemporânea depende cada vez mais de padrões que coordenam o comportamento sem substituir a autoridade

¹¹⁵ Ostrom, Elinor. "Polycentric Systems for Coping with Collective Action and Global Environmental Change." *Global Environmental Change* 20, no. 4 (2010): 550-557

¹¹⁶ Rolf H Weber, *Legal Interoperability as a Tool for Combatting Fragmentation* (Global Commission on Internet Governance Paper Series No 4, Centre for International Governance Innovation, December 2014); Luca Belli and Danilo Doneda, 'Data Protection in the BRICS Countries: Legal Interoperability through Innovative Practices and Convergence' (2023) 13(1) *International Data Privacy Law* 1–24; Luca Belli and Nathalia Foditsch, 'Network Neutrality: An Empirical Approach to Legal Interoperability' in Luca Belli and Primavera De Filippi (eds), *Net Neutrality: Competing Perspectives on Freedom of Expression Online* (Springer 2016) 281–298

jurídica doméstica.¹¹⁷ A interoperabilidade digital reflete exatamente essa dinâmica. Padrões comuns permitem que as instituições cooperem preservando a autonomia legal, desde que tais padrões permaneçam sujeitos à governança legítima e à responsabilidade democrática. A compatibilidade técnica sem autoridade jurídica pode facilitar o processamento ilegal de dados; a compatibilidade jurídica sem coordenação organizacional frequentemente permanece ineficaz; a cooperação organizacional sem coerência semântica pode gerar resultados administrativos incorretos; e a convergência conceitual sem implementação técnica permanece meramente aspiracional. Portanto, a governança de dados não deve ser vista como uma dimensão adicional de interoperabilidade, mas como o arcabouço normativo que permeia cada uma dessas dimensões.

A interoperabilidade deve, portanto, ser entendida não como o oposto da soberania, mas como uma de suas principais expressões operacionais. A interoperabilidade devidamente governada permite cooperação sem uniformidade institucional, coordenação sem centralização e abertura sem perda de controle democrático.¹¹⁸ Ele traduz a capacidade integrada de governança descrita na Seção III nas condições práticas de cooperação entre soberanos iguais desenvolvidas na Seção 4.1. No entanto, a interoperabilidade por si só permanece uma condição de interação legítima, e não uma capacidade institucional permanente. Para que a interoperabilidade governada se torne repetível, confiável e escalável, ela deve ser suportada por infraestruturas compartilhadas.

4.3. INFRAESTRUTURA PÚBLICA DIGITAL COMO FACILITADOR COMPARTILHADO

A seção anterior argumentou que a interoperabilidade é uma das principais expressões operacionais da soberania porque permite que instituições juridicamente autônomas cooperem sob regras compartilhadas sem abrir mão de seus mandatos ou autoridade decisória. Infraestrutura Pública Digital (DPI, acrônimo de *Digital Public Infrastructure*) ocupa o próximo passo nesse argumento. Se a interoperabilidade descreve as condições sob as quais sistemas e instituições

¹¹⁷ Kenneth W Abbott and Duncan Snidal, 'International "Standards" and International Governance' (2001) 8(3) *Journal of European Public Policy* 345–370; Kenneth W Abbott and Duncan Snidal, 'Strengthening International Regulation through Transnational New Governance: Overcoming the Orchestration Deficit' (2009) 42(2) *Vanderbilt Journal of Transnational Law* 501–578

¹¹⁸ Belli, L. and Bhinder, A. Cooperative Digital Sovereignty and Artificial Intelligence Promoting Resilience, Strategic Openness, and Self-Determination. (Digital Cooperation Organization, 2026).

podem interagir legitimamente, a DPI fornece as capacidades compartilhadas que tornam essa interação repetível, confiável e escalável.¹¹⁹ Portanto, não é uma alternativa paralela à interoperabilidade, mas o substrato infraestrutural por meio do qual a interoperabilidade governada se torna uma expressão duradoura da soberania cooperativa.

A interoperabilidade sozinha não cria cooperação; ela apenas possibilita a interação. A cooperação duradoura requer capacidades institucionais que possam ser reutilizadas em diversos serviços, setores e jurisdições. A DPI transforma a interoperabilidade de um conjunto de compatibilidades técnicas, semânticas, legais e organizacionais em uma capacidade pública persistente. Uma vez estabelecidos serviços comuns de confiança, estruturas de credenciais, *rails* de pagamento e mecanismos de troca de dados, novos serviços não precisam recriar as bases institucionais da cooperação. Em vez disso, a confiança se incorpora à infraestrutura por meio de níveis de garantia compartilhados, regras de procedência, mecanismos de auditoria, controles de acesso e estruturas de governança.

Essa função institucional é particularmente significativa em contextos transfronteiriços. Em uma economia digital caracterizada pela dependência de um número limitado de infraestruturas proprietárias, a DPI compartilhado oferece uma alternativa tanto à fragmentação quanto à dependência tecnológica. Ao depender de padrões abertos, arquiteturas modulares e *frameworks* de confiança governados publicamente, ele possibilita a cooperação sem exigir dependência de uma única plataforma ou provedor.¹²⁰ Essa abordagem fortalece tanto a autonomia institucional quanto a competição ao garantir que as capacidades digitais fundamentais permaneçam transparentes, interoperáveis, contestáveis e responsáveis, ao mesmo tempo em que deixa amplo espaço para inovação na camada de aplicação.

Portanto, o DPI contribui para a soberania dos dados apenas quando permanece modular, seguro, auditável, interoperável e substituível. Devidamente governado, ele conecta a interoperabilidade com uma concepção cooperativa de soberania digital¹²¹, permitindo que instituições autônomas autenticuem, troquem informações e forneçam serviços digitais sob arranjos de governança

¹¹⁹ Mila Samdub and Chand Rajendra-Nicolucci, 'What is Digital Public Infrastructure? Towards More Specificity' (*Tech Policy Press*, 25 November 2024); Mila T Samdub, '*Digital Public Infrastructure*' at a *Turning Point: From Definitions to Motivations* (Open Future, February 2025)

¹²⁰ Doctorow, C. (2021). *How to destroy surveillance capitalism*. Medium Editions.

¹²¹ Belli, L. and Bhinder, A. Cooperative Digital Sovereignty and Artificial Intelligence Promoting Resilience, Strategic Openness, and Self-Determination. (Digital Cooperation Organization, 2026).

compartilhada, preservando a diversidade jurídica, a responsabilidade democrática e a igualdade soberana das jurisdições participantes.

4.4. DA DEPENDÊNCIA À INTERDEPENDÊNCIA RESILIENTE

A estrutura desenvolvida ao longo deste capítulo leva, em última análise, a uma compreensão diferente da soberania dos dados como a capacidade institucional de governar a interdependência. O desafio central enfrentado pelos Estados contemporâneos, portanto, não é se os ecossistemas digitais devem ser abertos ou fechados, mas se a abertura pode ser governada de maneiras que preservem a agência democrática, a autonomia institucional e a responsabilidade constitucional.

Essa distinção é fundamental porque soberania raramente implicou autossuficiência completa. Os Estados modernos sempre dependeram do comércio, do intercâmbio científico, dos sistemas financeiros, das normas técnicas e das instituições internacionais. Sua soberania não dependeu da eliminação da interdependência, mas da participação em relações interdependentes sob condições de reciprocidade, autonomia institucional e escolha significativa. O mesmo princípio se aplica à economia digital.

A distinção relevante, portanto, não é entre abertura e soberania, mas entre dependência e interdependência resiliente. A dependência surge quando a vinculação a infraestruturas, tecnologias ou arranjos de governança externos restringe substancialmente a capacidade dos Estados e de suas instituições realizarem escolhas públicas legítimas. Um governo pode formalmente manter autoridade sobre seus dados, leis e instituições públicas sem ter capacidade efetiva para auditar sistemas críticos, substituir fornecedores, preservar a continuidade operacional, diversificar opções tecnológicas ou garantir que o valor econômico gerado por meio das atividades digitais contribua para o desenvolvimento interno. Dependência, portanto, não implica confiança; ao contrário, ela se caracteriza pela ausência de escolhas institucionais significativas.

A interdependência resiliente, por outro lado, é totalmente compatível com a soberania. Ela surge quando a cooperação é estruturada por meio de reciprocidade, transparência, contestabilidade, auditabilidade, reversibilidade, diversificação e confiança institucional.¹²² Nessas condições, os Estados permanecem conectados sem se tornarem cativos, abertos sem se tornarem subordinados e cooperativos sem

¹²² Belli, L. and Bhinder, A. Cooperative Digital Sovereignty and Artificial Intelligence Promoting Resilience, Strategic Openness, and Self-Determination. (Digital Cooperation Organization, 2026); Belli L. and others, Soberania Digital e Inteligência Artificial no Brasil: Rumo à autonomia tecnológica (Lumen-Juris 2026).

renunciar à autonomia constitucional. Portanto, uma relação digital deveria ser considerada soberana não por ser territorialmente fechada, mas porque preserva a capacidade de revisar escolhas tecnológicas, diversificar infraestruturas, aplicar salvaguardas legais, auditar sistemas, participar da criação de valor e contestar arranjos de governança ao longo do tempo.

O arcabouço integrado de governança desenvolvido neste documento explica como a agência pode ser sustentada. A governança constitucional e de dados estabelece a legitimidade jurídica e a alocação institucional de autoridade. A Infraestrutura Pública Digital fornece as capacidades institucionais compartilhadas por meio das quais a governança pode ser operacionalizada. A interoperabilidade permite que instituições e jurisdições autônomas cooperem por meio de padrões comuns e arranjos de governança confiáveis, preservando seus respectivos mandatos. A cibersegurança protege a integridade e a confiabilidade das infraestruturas compartilhadas. Políticas industriais e de concorrência preservam a capacidade tecnológica, a inovação e a escolha estratégica, enquanto a capacidade fiscal garante que esses arranjos permaneçam financeiramente e institucionalmente sustentáveis. Juntas, essas dimensões constituem as condições institucionais pelas quais a soberania pode ser exercida dentro de sociedades digitalmente interconectadas.

As implicações vão além da governança de dados. A soberania no ecossistema digital não pode mais ser avaliada exclusivamente por meio da jurisdição territorial, propriedade de infraestrutura ou localização de dados. Também deve ser avaliada de acordo com a capacidade institucional dos Estados para moldar as condições tecnológicas, jurídicas e econômicas sob as quais a transformação digital se desenrola.¹²³ Portanto, a soberania dos dados não deve ser entendida como a capacidade de impedir que dados cruzem fronteiras, nem como a busca pela autarquia tecnológica. É a capacidade institucional de determinar as condições constitucionais, legais, tecnológicas e econômicas sob as quais dados, autoridade pública e confiança institucional podem circular legitimamente entre ecossistemas digitais interconectados.

CONCLUSÕES

Este estudo argumenta que soberania de dados não deve ser entendida como controle territorial sobre os dados, nem como sinônimo de localização de dados. Também não deve ser reduzido à proteção de informações pessoais, por mais fundamental que esse objetivo permaneça. Em vez disso, a soberania dos dados deve ser entendida como a capacidade institucional de indivíduos, sociedades e estados

¹²³ Idem.

para governar a geração, processamento, troca e uso de dados de acordo com objetivos democraticamente legítimos. Importante destacar que essa capacidade não decorre de nenhum instrumento jurídico ou solução tecnológica isolada. Ela surge da interação de múltiplas capacidades de governança que, juntas, permitem que as sociedades exerçam uma agência significativa dentro de uma economia digital cada vez mais interconectada.

O texto, portanto, propôs expandir a doutrina clássica da autodeterminação informativa. A evolução histórica dessa doutrina demonstra sua importância duradoura. Começando com a Decisão do Censo do Tribunal Federal Alemão e posteriormente desenvolvendo-se por meio do direito constitucional europeu, da jurisprudência do Tribunal Interamericano de Direitos Humanos, das estratégias de desenvolvimento asiáticas e da pesquisa pós-colonial africana, a autodeterminação informativa consolidou-se como uma base normativa indispensável para a governança digital ao proteger a dignidade humana, a autonomia pessoal e a participação democrática. Esses valores permanecem tão essenciais hoje quanto há quatro décadas.

No entanto, a economia digital contemporânea apresenta desafios que vão muito além da relação entre indivíduos e aqueles que tratam as suas informações pessoais. Sistemas de inteligência artificial dependem de volumes sem precedentes de dados. A computação em nuvem transformou infraestruturas digitais em ecossistemas distribuídos globalmente. Operações cibernéticas estão cada vez mais direcionadas a serviços públicos críticos. Um número relativamente pequeno de corporações exerce influência significativa sobre serviços em nuvem, plataformas digitais, sistemas operacionais móveis e modelos fundamentais de IA. Ao mesmo tempo, a competição geopolítica se intensificou em torno de semicondutores, infraestrutura de telecomunicações, ecossistemas de software e sistemas de pagamento digital. Os dados tornaram-se não apenas objetos de proteção jurídica, mas recursos estratégicos cuja governança molda cada vez mais o desenvolvimento econômico, a inovação tecnológica e a resiliência nacional.

Essas transformações exigem um arcabouço conceitual mais amplo, onde a autodeterminação informativa continua necessária, mas já não é suficiente. No artigo, portanto, argumentou-se que a soberania dos dados deveria ser entendida como um arcabouço multidimensional de governança constituído por seis capacidades de reforço mútuo: a proteção dos direitos fundamentais por meio da proteção de dados; cibersegurança e resiliência digital; governança tecnológica por meio da Infraestrutura Pública Digital; desenvolvimento industrial e capacidade tecnológica; competição e inovação; e justiça fiscal por meio da distribuição equitativa do valor gerado pelos dados. Cada uma dessas dimensões aborda uma fonte distinta de vulnerabilidade dentro dos ecossistemas digitais contemporâneos. Nenhum, no entanto, pode produzir soberania de forma independente. Somente a interação deles cria as condições institucionais pelas quais uma governança significativa se torna possível.

No capítulo também se argumentou que a soberania dos dados possui uma dimensão internacional essencial. A economia digital é inerentemente transnacional. Computação em nuvem, desenvolvimento de software, inteligência artificial, comércio digital e redes de comunicação dependem de formas de cooperação que nenhum país pode realisticamente substituir por meio de autossuficiência tecnológica completa. O desafio enfrentado pelos Estados não é, portanto, como eliminar a interdependência, mas como evitar que a interdependência se torne dependência estrutural.

Essa distinção ganhou maior relevância nos últimos anos. A crescente fragmentação do sistema internacional demonstrou que infraestruturas tecnológicas e financeiras podem se tornar instrumentos de influência geopolítica. Controles de exportação de semicondutores avançados, restrições que afetam serviços em nuvem, limitações ao acesso a tecnologias digitais e o uso estratégico de infraestruturas financeiras e tecnológicas ilustraram que a dependência de ecossistemas digitais externos pode restringir significativamente a margem de escolha dos Estados na formulação e implementação de suas políticas.

Nesse contexto, a conclusão deste capítulo é que a soberania dos dados não deve ser equiparada ao isolacionismo digital. Tentativas de isolar os ecossistemas digitais nacionais da cooperação internacional não apenas seriam economicamente custosas, mas também minariam muitos dos benefícios gerados pela colaboração científica global, pelo comércio digital e pela inovação tecnológica. Igualmente, porém, a dependência irrestrita de um número limitado de infraestruturas digitais estrangeiras corre o risco de criar assimetrias estruturais incompatíveis com uma igualdade soberana significativa.

A alternativa proposta neste documento é a soberania cooperativa. Construir soberania de dados requer cooperação fundamentada em conceitos compartilhados, padrões técnicos interoperáveis, marcos jurídicos compatíveis, arquiteturas de cibersegurança confiáveis e princípios institucionais comuns. A soberania é, portanto, fortalecida quando os Estados cooperam para desenvolver infraestruturas públicas digitais abertas, coordenar padrões de cibersegurança, estabelecer mecanismos confiáveis para a governança transfronteiriça de dados e promover a participação equitativa na economia digital.

O caminho à frente, no entanto, continua desafiador. Os ecossistemas digitais contemporâneos persistem caracterizados por uma concentração significativa de capacidade tecnológica, poder de mercado e controle de infraestrutura. Os enormes investimentos necessários para semicondutores avançados, computação em nuvem em hiperescala, inteligência artificial de vanguarda e redes globais de comunicação criam barreiras que poucos países conseguem superar de forma independente. Os incentivos econômicos que favorecem a concentração continuam fortes, enquanto a competição geopolítica se intensifica. Nessas condições, a aspiração à soberania dos dados não deve ser confundida com a ilusão de completa independência tecnológica.

Em vez disso, o objetivo deve ser fortalecer progressivamente a capacidade de governança por meio da construção institucional. Investimentos em infraestrutura pública digital, cibersegurança, habilidades digitais, ecossistemas de inovação doméstica, padrões abertos e cooperação regional podem gradualmente reduzir dependências estruturais, preservando os benefícios de uma economia digital aberta. Países de renda média e em desenvolvimento, em particular, dificilmente alcançarão soberania digital significativa atuando isoladamente. A cooperação entre países que enfrentam desafios de desenvolvimento semelhantes torna-se, portanto, não apenas desejável, mas estrategicamente necessária.

Em última análise, a soberania sempre evoluiu junto com as transformações na organização do poder político e econômico. O surgimento do Estado territorial redefiniu a soberania durante o período moderno inicial. A industrialização a transformou novamente ao vincular a autoridade política à capacidade econômica e tecnológica. Hoje, a revolução digital está gerando uma transformação comparável. No século XXI, a soberania é cada vez mais exercida por meio da governança dos dados, algoritmos, infraestruturas digitais e das instituições que os sustentam.

O argumento central deste artigo pode, portanto, ser anunciado de forma simples. Construir soberania de dados requer expandir o alcance da autodeterminação informativa para além de suas bases individualistas tradicionais para abranger cibersegurança, infraestrutura pública digital, desenvolvimento industrial, competição, justiça fiscal e cooperação internacional. Somente por meio desse quadro multidimensional a transformação digital será possível contribuir não apenas para o crescimento econômico, mas igualmente para a dignidade humana, a resiliência democrática e desenvolvimento sustentável.