

**The Future of Data Governance for Development:
A Report on Cross-cutting Issues for the UN CSTD Working Group on Data Governance**

Applied Research Project 2025-2026: Final Report

Matteo Bovarini
Jessica Johnson
Bessie Qu
Clémence Vergé

12 May 2026

TABLE OF CONTENTS

1. Website	
1.1. Access to Applied Research Project Website.....	2
2. Overview	
2.1. Historical Context of Data Governance.....	3
2.2. Geographical Scope.....	4
2.3. Importance of the Working Group Process.....	7
3. Literature Review	
3.1. Conceptual Foundations.....	9
3.2. Operational and Technical Foundations.....	10
3.3. Cross-cutting Gaps.....	11
4. Analytical Brief: Reconciling Sovereignty and Interoperability in Data Governance	
4.1. Introduction.....	13
4.2. Sovereignty as Authority over Underlying Interests.....	14
4.3. Interoperability as a Governance Mechanism for Managing Sovereignty Claims.....	18
4.4. Policy Implications.....	21
4.5. Looking Ahead.....	22
5. Thematic Articles	
5.1. From Policy to Public, from Public to Policy: Making Data Governance Legible in the Digital Age.....	23
5.2. Whose Cloud, Whose Coffee? Designing Data Governance towards a 'Right to Knowledge' in Agrifood Systems.....	29
5.3. Strengthening Indigenous Data Sovereignty and Knowledge Co-production: Addressing Inequalities in Global Data Governance.....	33
5.4. Embedding Human Rights and Data Justice in Health Data Governance.....	39
6. Data Visualizations	
6.1. Analysis of Key Terms Across Working Group Submissions.....	45
6.2. Data Openness, Human Development, and Rule of Law.....	56
7. References	
7.1. Bibliography.....	58

1. WEBSITE

1.1 Access to Applied Research Project Website

This project started from a simple observation; while data governance is increasingly central to development, it remains fragmented, complex and inaccessible to the broader public. This is why we decided to build a website named *“The Future of Data Governance For Development”* in order to:

- 1) Analyze and structure the debates emerging from the UN Commission on Science and Technology for Development (CSTD) Working Group on Data Governance;
- 2) Make these debates more legible both analytically and visually.

To achieve these objectives, our website encompasses a multi-layered approach that combines data visualizations, a background and literature review, an analytical brief and applied case studies. For academic purposes the full contents of the website are reproduced in this report.

For direct access to the online platform, please visit: <https://datagovernancearp.wixstudio.com/iheid>.

2. OVERVIEW

2.1 Historical context of data governance

The early foundations of data governance date back to the 1960s, when organizations began adopting databases and computers. Since then, data governance has evolved with the role data played within organizations, the economy, and society. During the first phase, data was initially seen as an operational product within organizations, and its governance was mostly informal and centered on technical management. In the 1980s, the rise of enterprise databases introduced the need for data quality, metadata and access controls. In *Data Governance as a Collective Action Problem*, Olivia Benfeldt, John Stouby Persson and Sabine Madsen highlight how organizations had to reorganize themselves in response to growing inconsistencies between data systems, which created increasing risks for businesses.¹ Companies thus slowly started to experiment with structured data management frameworks, even though they initially faced practical and organisational challenges.

During the second phase, regulators became more aware of the cumulative effects of enterprise-level governance frameworks and called for greater standardisation across the board. Major events such as the Enron fraud scandal (2001) and the subsequent enactment of the Sarbanes-Oxley Act (2002) promoted stricter accountability regulations and practices, expanding data governance beyond technical administration towards broader concerns around risk management, transparency, and corporate responsibility.² Subsequently, data governance became more of a society-level concern with growing collective interest in protecting data privacy and security. The research study *Mapping the evolution of data governance* by Hossein Hassani, Xu Huang and Steve MacFeely emphasizes how the explosion of big data, cloud computing and artificial intelligence (AI) made global data governance crucial for transparency and development.³ Organizations shifted from a compliance-driven approach to more value-driven governance models intended to balance regulations with innovation.

A key contributor to this agenda is the United Nations Conference on Trade and Development: Commission on Science and Technology for Development (UNCTAD CSTD) Working Group on Data Governance (the Working Group), created in 2024 following the UN Summit of the Future. The Working Group represents a multi-stakeholder initiative designed to foster dialogue on data governance at all levels. The initiative aims to move from fragmented national, regional and international approaches towards a common framework with shared principles, interoperable practices and ultimately a responsible, inclusive and development-oriented data environment.

The Summit of the Future outcome document also contained the Global Digital Compact (the GDC) which sets forth a comprehensive framework for digital cooperation.⁴ Under the mandate of GDC,

¹ Benfeldt, Olivia, John Stouby Persson, and Sabine Madsen. *Data Governance as a Collective Action Problem*. *Information Systems Frontiers*, vol. 22, no. 2 (2020): 299–313. <https://doi.org/10.1007/s10796-019-09923-z>.

² Enron (2001): The auditing company Enron was involved in bankruptcy and accounting frauds, generating global debates and legislation designed to improve accounting standards and practices. Sarbanes-Oxley Act (2002): Law passed by the US Congress to protect investors from fraudulent financial reporting by companies.

³ Hassani, Hossein, Xu Huang, and Steve MacFeely. "Mapping the Evolution of Data Governance Scientific Research." *Data & Policy* 7 (2025): e51. <https://doi.org/10.1017/dap.2025.10014>.

⁴ United Nations. "Global Digital Compact:" the official compact as adopted as part of the Pact for the Future at the Summit of the the Future (22 September 2024). https://www.un.org/global-digital-compact/sites/default/files/2024-09/Global%20Digital%20Compact%20-%20English_0.pdf.

the Working Group approaches global data governance for development as a holistic framework involving public policies, standards and ethical safeguards to ensure that all member states can benefit from the value produced by data. In this context, the Working Group plays a key role in informing and reporting to the GDC process, providing analysis and stakeholders inputs to support its implementation and evolution. It responds to increasing concerns regarding unequal access to data, disparities in capabilities, as well as the concentration of power in the hands of a small number of actors, especially private companies.

2.2 Geographical scope

The governance of data remains deeply fragmented at the global level and is heavily influenced by political and legal systems, economic models, infrastructure capacity and geopolitical priorities. *The Geopolitics of Data Governance* by Christine Jiang and Sabrina Martin identifies three dominant models of data governance, each with additional regional variations.⁵ The differences between the models form the foundation of divergences within global data governance.

The European Union (EU) relies on a rights-based regulatory framework for data governance that prioritizes fundamental rights and human protection. Key legal instruments include the General Data Protection Regulation (GDPR),⁶ the EU Data Act,⁷ and the Data Governance Act.⁸ Together, these legal instruments aim to establish stricter privacy rules, conditions for cross-border data flows, data minimization obligations, and interoperability for public services and digital markets. The GDPR continues to influence data protection approaches in many regions, a phenomenon commonly described as the “Brussels effect.”

Alternatively, the market-driven model characteristic of the United States views data as an economic asset shaped by innovation and competition. There is no national regulatory framework, and the governance of data relies largely on sectoral privacy laws, such as the Children’s Online Privacy Protection Act (COPPA),⁹ the Financial Services Modernization Act of 1999 (GLBA),¹⁰ and the Health Insurance Portability and Accountability Act (HIPAA).¹¹ These laws support open data flows while providing sector-specific protections, safeguards, and a regulatory environment conducive to innovation. It is worth noting that Canada, while economically integrated with the U.S., has adopted a more rights-based data protection regime that more closely resembles the EU model through instruments such as the Personal Information Protection and Electronic Documents Act (PIPEDA) and related reforms.¹²

⁵ Jiang, Christine J., and Sabrina Martin. *The Geopolitics of Data Governance Research Report Part I: Data Governance Regimes*. Oxford Insights, May 2020. https://oxfordinsights.com/wp-content/uploads/2024/08/The-Geopolitics-of-Data-Governance_Oxford_insights_Master.pdf.

⁶ General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

⁷ EU Data Act: Regulation (EU) 2023/2854 of the European Parliament and of the Council of 27 November 2023 on harmonised rules on fair access to and use of data.

⁸ Data Governance Act: Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act).

⁹ Children’s Online Privacy Protection Act (COPPA): Imposes regulations on how websites and online services collect data from young children under 13.

¹⁰ Financial Services Modernization Act of 1999 (GLBA): Act protecting sensitive data of users.

¹¹ Health Insurance Portability and Accountability Act (HIPAA): Act passed by the US Congress to protect health data and life privacy of health patients.

¹² Personal Information Protection and Electronic Documents Act (PIPEDA), S.C. 2000, c. 5 (Canada).

Lastly, the third dominant framework is a state-centric model, most clearly represented by China, which treats data as a strategic resource for national security and economic planning. The party-state strictly exercises oversight over data access, transfer, and classification through a suite of laws and regulations, including the Data Security Law (DSL)¹³ and the Cybersecurity Law (CSL).¹⁴ China maintains one of the strictest cross-border data transfer regimes globally and is developing new digital public infrastructures, including the recently announced National Data Administration.¹⁵

One way to see how these models materialize in practice is to look at the extent to which they influence how particular regions selectively combine, adapt, or contest them in light of their own political economies, security concerns, and development priorities.

A policy brief from the Robert Schuman Centre, “Data governance models and geopolitics: Insights from the Indo-Pacific region,” highlights diverse data policies and emerging patterns of data governance across the region.¹⁶ East Asia generally adopts mixed models that integrate rights, markets and state interests. Japan operates a hybrid framework combining strong privacy protections with pro-innovation policies and high interoperability. Similarly, South Korea has a robust privacy regime under the Personal Information Protection Act (PIPA)¹⁷ and is increasingly aligned with EU adequacy standards.

South Asia is a fast-developing region seeking to balance development priorities with sovereignty considerations, with individual countries operating under varying technological and institutional capacities. India is expanding its digital public infrastructure, seen for example with its Open Network for Digital Commerce (ONDC),¹⁸ and adopted a new privacy framework, the Digital Personal Data Protection Act, in 2023.¹⁹ Other South Asian countries, such as Sri Lanka, Pakistan and Bangladesh, are developing privacy frameworks inspired by the European model, with implementation capacity influenced by each country’s institutional and technological landscape.²⁰

The Southeast Asia region remains highly diverse despite efforts to harmonize digital rules, including through the recently adopted ASEAN Digital Economy Framework Agreement (DEFA).²¹ Singapore is a

¹³ Data Security Law (DSL): Data Security Law of the People’s Republic of China, adopted at the 29th meeting of the Standing Committee of the 13th National People’s Congress on 10 June 2021, effective 1 September 2021.

¹⁴ Cybersecurity Law (CSL): Cybersecurity Law of the People’s Republic of China, adopted at the 24th meeting of the Standing Committee of the 12th National People’s Congress on 7 November 2016, effective 1 June 2017.

¹⁵ Beijing Post. “China’s Digital Landscape: A Comprehensive Overview of ‘Digital China’ Initiatives.” Beijing Post, November 21, 2025. <https://beijingpost.com/china-s-digital-landscape-a-comprehensive-overview-of-digital-china-initiatives>.

¹⁶ Ferracane, Martina Francesca. Data Governance Models and Geopolitics: Insights from the Indo-Pacific Region. Policy Briefs, 2022/48, Global Governance Programme. European University Institute, 2022. <https://cadmus.eui.eu/server/api/core/bitstreams/d76f633f-0ab8-5eb5-a876-8984917dae6e/content>.

¹⁷ Personal Information Protection Act (PIPA) (Act No. 10465), enacted 29 March 2011, as amended (latest major amendment: 2023).

¹⁸ ONDC (Open Network for Digital Commerce). ONDC Network Policies and Documentation. 2024. <https://www.ondc.org/rfp/>.

¹⁹ Digital Personal Data Protection Act, 2023: The Digital Personal Data Protection Act, 2023, No. 22 of 2023, enacted by the Parliament of India, 11 August 2023.

²⁰ Bentotahewa, Vibhushinie, Chaminda Hewage and Jason Williams. “The Normative Power of the GDPR: A Case Study of Data Protection Laws of South Asian Countries,” *SN Computer Science* 3, no. 3 (2022): 183, <https://doi.org/10.1007/s42979-022-01079-z>.

²¹ ASEAN Secretariat; Boston Consulting Group; Australian Government (Australia for ASEAN Futures Economic and Connectivity). 2024. *Study on the ASEAN Digital Economy Framework Agreement (DEFA), Public Version 2.0*. November 8, 2024.

regional leader in promoting data openness and trusted cross-border data flows, while countries such as Malaysia and the Philippines have established comparatively strong privacy frameworks.²²

The Middle East is playing a growing role in advancing digital governance, with investments in national data strategies, digital public services and innovative projects such as smart city developments. Driven by rapid modernization, the Gulf States are focusing on digital state-building, combining state oversight with investment in data protection. Many have adopted national data strategies that emphasize AI development, open data initiatives and cloud computing.²³

Latin America has emerged as a regional leader in rights-focused data governance with a particular emphasis on digital trust and data openness. Brazil's General Data Protection Law (LGPD)²⁴ exemplifies a robust privacy framework, while other countries such as Chile, Colombia and Argentina are committing to major reforms to modernize their data protection regimes.²⁵

Africa faces the challenge of balancing development goals with regulatory capacity. Pan-African initiatives such as the Smart Africa Alliance (2013) and the Malabo Convention (2014) support harmonization efforts for a more integrated data market.²⁶ Regional blocs, such as the South African Development Community (SADC) and the Economic Community of West African States (ECOWAS) have advanced cybersecurity, privacy and data protection frameworks. The African Union's Data Policy Framework (2022)²⁷ and the African Digital Compact (ADC)²⁸ represent major steps towards more coordinated governance addressing the continent's specific challenges. At the national level, regulatory frameworks for data governance vary. For instance, South Africa established a strong rights-based model through the Protection of Personal Information Act (POPIA, 2013)²⁹ while Nigeria and Kenya are emerging as digital hubs with more flexible regulatory modes.³⁰

At the international level, global organizations and transnational initiatives play a crucial role in driving convergence and reducing fragmentation caused by diverging national laws. To the extent that convergence is a desirable aim, this level of governance represents perhaps the only viable path toward coherent and enforceable global standards. Two distinct categories of governance mechanisms are at work here, each with different implications for this process.

²² See, for example, United Nations Conference on Trade and Development (UNCTAD). *Digital Economy Report 2021: Cross-border Data Flows and Development—For Whom the Data Flow?* Geneva: United Nations, 2021, and UNCTAD. *Summary of Adoption of E-Commerce Legislation Worldwide*. UNCTAD Global Cyberlaw Tracker. <https://unctad.org/topic/ecommerce-and-digital-economy/ecommerce-law-reform/summary-adoption-e-commerce-legislation-worldwide>.

²³ Gulf News Report. "How AI, Data Sovereignty and Open Source Are Redefining Leadership in the Middle East." Gulf News, February 11, 2025. <https://gulfnews.com/business/how-ai-data-sovereignty-and-open-source-are-redefining-leadership-in-the-middle-east-1.500033816>.

²⁴ Brazilian General Data Protection Law (LGPD): Lei No. 13.709, de 14 de Agosto de 2018, amended by Law No. 13.853/2019.

²⁵ Crowell & Moring LLP. "Latin American Data Privacy." Crowell & Moring Insights, January 28, 2025. <https://www.crowell.com/en/insights/publications/latin-american-data-privacy>.

²⁶ African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), adopted in Malabo, Equatorial Guinea, on 27 June 2014.

²⁷ African Union Commission. *African Union Data Policy Framework*. Addis Ababa: African Union, 2022.

²⁸ African Union. *African Digital Compact (ADC)*. 9 August 2024. African Union Commission.

²⁹ Protection of Personal Information Act (POPIA): Act 4 of 2013, assented to 19 November 2013, with most provisions effective 1 July 2020.

³⁰ See, for example, the International Telecommunication Union's (ITU) publications: *Collaborative Regulation: Accelerating Nigeria's Digital Transformation*. 2023. and *Collaborative Regulation for Digital Transformation in Kenya: A Country Review*. 2023.

The first encompasses trade agreements and other arrangements negotiated between smaller groups of UN member states. Several such agreements incorporate cross-border data flow standards, including the United States-Mexico-Canada Agreement (USMCA)³¹, the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP)³², and the Digital Economy Partnership Agreement (DEPA).³³ Regional initiatives such as the Asia-Pacific Economic Cooperation (APEC) and the Cross-Border Privacy Rules (CBPR) System similarly foster interoperability across differing legal systems.³⁴ Notably, these frameworks cover only a subset of UN member states, leaving a significant number of countries outside any ongoing processes in this area.

The second category involves norm and standard-setting efforts led by UN bodies and broader international organizations. The Organisation for Economic Co-operation and Development (OECD) influences policy across North America, the EU and other member states by promoting high-level governance and privacy principles. International organizations such as the International Telecommunication Union (ITU), the United Nations Educational, Scientific and Cultural Organization (UNESCO), and various other UN bodies are actively developing principles for data ethics, responsible data sharing, and digital cooperation.

The geographical scope of data governance is thus characterized by diverse political strategies, economic priorities and legal systems. The world is increasingly coalescing around three digital blocs shaped by the EU rights-based model, the US market-driven model and the Chinese state-centric model. Other regions navigate among these models, adapting them to local needs, development goals and geopolitical priorities.

However, a certain level of fragmentation in regulatory frameworks for data governance is expected to persist. Given how fragmentation impacts global business operations and affects development outcomes, it is all the more important to identify a set of common principles and practices. These commonalities can in turn provide an evidence-based foundation for more effective cooperation despite different governance approaches. Emerging digital blocs shape norms, infrastructure, and systems, which in turn influence how new political and economic partnerships are formed. Interoperability is then further challenged as standards and regulatory requirements diverge, generating friction of cross-border data transfers with impact on global trade and supply chains.

Therefore, as digital systems are becoming increasingly interconnected but legally fragmented, understanding and mapping this geographical diversity is crucial for the Working Group to establish fundamental principles for interoperability, benefit sharing and cross-border data flows.

2.3 Importance of the Working Group Process

In recognition of the importance of responsible and interoperable data governance in advancing development objectives, protecting human rights, fostering innovation and promoting economic growth, the Working Group was established to engage in a comprehensive and inclusive

³¹ United States–Mexico–Canada Agreement (USMCA), signed 30 November 2018, entered into force 1 July 2020.

³² Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP): signed 8 March 2018, entered into force 30 December 2018.

³³ Digital Economy Partnership Agreement (DEPA): signed 2020 by Chile, New Zealand, and Singapore, entered into force 7 January 2021.

³⁴ APEC Cross-Border Privacy Rules (CBPR) System: Launched by APEC in 2011, governed by the APEC Privacy Framework (2005, revised 2015).

multi-stakeholder dialogue on data governance at all levels as relevant for development.³⁵ In line with its mandate under the Global Digital Compact (GDC), the Working Group is also tasked with reporting to and informing the GDC process, bringing together stakeholders perspectives and policy recommendations to support its implementation.

Despite the widespread recognition of data as a strategic resource, the global data governance landscape is currently marked by divergent legal frameworks and uneven technological and institutional capacities, both of which are exacerbated by differing political and economic priorities. The extent of fragmentation creates challenges for interoperability, hinders cross-border data flows and reinforces existing inequalities in the digital economy.

A key priority identified in the Global Digital Compact is the need for international cooperation that closes all digital divides between and within countries.³⁶ In the context of data governance, it means the need for identifying areas of convergence, shared indicators and strengthened cooperation across national, regional and international levels. Efforts to enhance interoperability, promote responsible data sharing and develop trusted data infrastructures can help reduce barriers, foster innovation and support the use of data for the public good. At the same time, bridging digital divides, including disparities in skills, infrastructure, institutional capacity and access to datasets, is crucial for ensuring that the benefits of the data-driven economy are equitably distributed.

Given this context, our research project contributes new insights supporting the deliberations of the Working Group by synthesizing existing literature, policy frameworks and debates across the Working Group's four thematic tracks:

1. Fundamental principles of data governance relevant for development
2. Proposals to support interoperability between national, regional and international data systems
3. Considerations of sharing the benefits of data
4. Options to facilitate safe, secure and trusted cross-border data flows relevant for development

Throughout our work, we consider how the contributions of the Working Group align with global discussions on data governance, current policy trends and emerging developmental priorities. Our goal is to provide evidence-based inputs that can support the Working Group's efforts to identify areas of convergence and contribute toward a global consensus across these four themes.

³⁵ Global Digital Compact, *supra* note 4, paragraph 48.

³⁶ *Ibid*, paragraph 2.

3. LITERATURE REVIEW

Our literature review establishes the conceptual and narrative building blocks of data governance. In the first body of literature, we analyze the conceptual framework of the nature of data, the challenges of governing data across jurisdictions and related equity considerations. We have also reviewed a significant body of literature on operationalizing data governance frameworks and related limitations. We conclude our review by surfacing gaps in existing academic and policy discussions as they relate to the mandate of the Working Group and explore how such analysis helps situate our work going forward.

3.1 Conceptual foundations

Understanding global data governance requires moving beyond the assumption that data is a purely technical or neutral artefact. Literature shows that data is shaped by institutional practices, cultural meanings, and social norms, rather than simply existing as raw inputs for computational systems.³⁷ This perspective highlights how data reflects embedded classifications, assumptions, and power structures that in turn influence how it is produced, accessed, stored and processed. Related research further highlights that data functions as an organizing force that restructures institutional boundaries and redistributes knowledge, giving rise to increasingly “decentred” and networked forms of governance even though such trends did not prevent market concentration.³⁸ This reframing is particularly insightful for global data governance as it underscores the fluidity and transnational nature of data, qualities that make traditional governance models inadequate.³⁹ They further inform policymakers that governance solutions must take into account the social and organizational environment in which data governance operates.

Another body of work focuses on the challenges of governing cross-border data flows, which often involves balancing national sovereignty considerations with the need for shared standards and interoperable systems. This inherent tension between the desire for state control over digital infrastructure and the economic and societal benefits of cross-border data exchange is well articulated in relevant literature.⁴⁰ Proposed governance models designed to bridge disparate legal and political systems rely on a layered approach that respects local autonomy while anchoring cooperation in shared international norms.⁴¹ For example, complementary legal research on sovereignty in cyberspace suggests that authority operates across overlapping “layers” of the digital ecosystem, with the possibility of states exercising different forms of sovereignty over each layer depending on the technical, legal and infrastructural mechanisms available to it.⁴² These conceptual models underscore why trust, sovereignty, and interoperability remain central in data governance.

³⁷ Aaltonen, Aleksi et al., “What Is Missing from Research on Data in Information Systems? Insights from the Inaugural Workshop on Data Research.” *Communications of the Association for Information Systems* 53 (2023): 475–90. <https://doi.org/10.17705/1CAIS.05320>.

³⁸ Alaimo, Cristina, and Jannis Kallinikos. “Organizations Decentered: Data Objects, Technology and Knowledge.” *Organization Science* 33, no. 1 (2022): 19–37. <https://doi.org/10.1287/orsc.2021.1552>.

³⁹ *Ibid.*

⁴⁰ Ishkhanyan, Artur. “The Sovereignty–Internationalism Paradox in AI Governance: Digital Federalism and Global Algorithmic Control,” *Discover Artificial Intelligence* 5 (2025): 123, <https://doi.org/10.1007/s44163-025-00374-x>.

⁴¹ *Ibid.*

⁴² Roguski, Piotr. “Layered Sovereignty: Adjusting Traditional Notions of Sovereignty to a Digital Environment.” In *11th International Conference on Cyber Conflict: CyCon*, edited by Tomáš Minárik, et al., 347–359. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2019.

A further body of literature examines data governance through the lens of equity, representation, and global power relations. These contributions emphasize that fairness in digital systems requires attention not only to privacy but also to structural forms of visibility, discrimination, and exclusion.⁴³ Analyses of digital political systems show how data-driven architectures can exacerbate existing inequalities in participation, raising concerns about concentration of power and uneven informational ecosystems.⁴⁴ Power imbalance is also created by infrastructural dependencies where developing countries rely on foreign-owned digital platforms and cloud systems, limiting their ability to assert digital sovereignty or capture the developmental value of their own data.⁴⁵ These perspectives reinforce the importance of development-oriented governance arrangements that support cross-border data flows while prioritizing national development priorities.

Taken together, these conceptual foundations underscore that data governance is an inherently political, institutional, and developmental challenge. The literature demonstrates that data practices are shaped by meaning, power, and capacity; that sovereignty and interoperability are difficult to reconcile; and that global asymmetries fundamentally structure who benefits from digital transformations. While these analyses offer valuable insights, they remain primarily conceptual, leaving open how these ideas can be translated into concrete institutional arrangements.

3.2 Operational and technical foundations

In addition to conceptual debates, a significant body of theoretical and empirical literature examines the operational and technical foundations of data governance. These works highlight the practical challenges that arise when translating principles into functioning systems, particularly in a fragmented governance environment. A key insight is that effective data governance requires navigating tensions between openness and protection, balancing regulatory overlap, and creating incentives for responsible data re-use.⁴⁶ Frameworks developed for policymaking emphasize that these tensions cannot be resolved through legal rules alone; they require a combination of shared technical standards, interoperable architectures, clear institutional responsibilities, and meaningful multi-stakeholder engagement.⁴⁷

Economic perspectives further illuminate how institutional and market structures shape the flow and use of data. Analyses of emerging data markets show that governance arrangements, whether highly liberalized or tightly regulated, strongly influence incentives for data exchange, access, and aggregation.⁴⁸ These dynamics have implications not only for interoperability but also for sharing the benefits of data, as they determine who can participate in data-driven value creation and under what conditions. However, these models often assume relatively mature digital economies and overlook the structural power asymmetries that limit participation for many lower-income countries, for which compliance costs are much higher.

⁴³ Taylor, Linnet. "What Is Data Justice? The Case for Connecting Digital Rights and Freedoms Globally." *Big Data & Society* 4, no. 2 (2017): 1–14. <https://doi.org/10.1177/2053951717736335>.

⁴⁴ Jungherr, Andreas. "Artificial Intelligence and Democracy: A Conceptual Framework." *Social Media + Society* 9, no. 3 (2023): 1–14. <https://doi.org/10.1177/20563051231186353>.

⁴⁵ Kwet, Michael. "Digital Colonialism and Infrastructure-as-Debt." *Frontiers in African Digital Research* 9 (2021): 66–72. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4004594.

⁴⁶ Organisation for Economic Co-operation and Development (OECD). *Going Digital: Guide to Data Governance Policy Making*. Paris: OECD Publishing, 2022.

⁴⁷ *Ibid.*

⁴⁸ Koutroumpis, Pantelis, Aija Leiponen, and Leonard D. Thomas. "Markets for Data." *Industrial and Corporate Change* 29, no. 3 (2020): 645–60.

Empirical assessments of global governance frameworks reinforce these concerns. Comparative analyses of existing national and international frameworks reveal considerable conceptual convergence around broad principles, such as transparency, accountability, and human-rights alignment, but persistent gaps in operational coherence.⁴⁹ Frameworks vary widely in maturity, institutional capacity, and scope, resulting in inconsistent implementation.⁵⁰ Other studies underscore the need for stronger international coordination mechanisms, shared standards, and ethical guidelines to address systemic fragmentation.⁵¹ However, these assessments tend to map divergences rather than propose concrete pathways for harmonization, and they rarely account for the institutional realities of developing countries or the practical constraints of multilateral processes.

Taken together, the operational literature highlights a recurring challenge: while a wide range of tools and frameworks exist for designing interoperable and trustworthy data ecosystems, they often assume capacities, infrastructures, and governance conditions that are not universally available. As a result, lower-income countries risk being left out of emerging governance arrangements or dependent on external systems and standards. This reinforces the importance of the Working Group's development-oriented mandate and underscores the need for governance models that are not only technically sound but also adaptable to diverse institutional contexts.

3.3 Cross-cutting gaps

Across the diverse body of literature on data governance, several cross-cutting gaps emerge. One of them is the divide between normative ambitions and technical implementation. Conceptual analyses emphasize values such as justice, sovereignty, equity, and accountability, yet they offer limited guidance on how these commitments can be translated into actual governance mechanisms or cross-border coordination structures.⁵² Conversely, operational literature provides detailed tools for interoperability, standard-setting, and regulatory design, but often treats equity, ethical concerns, and power asymmetries as secondary.⁵³

A second gap concerns the limited representation of developing country perspectives. While the literature acknowledges global disparities in data access and institutional capacity, very few studies examine how governance frameworks function in developing contexts or how value from data can be equitably redistributed.⁵⁴ Even empirical studies mapping global frameworks tend to focus on documenting variation rather than analyzing how different governance regimes impact countries with constrained resources or reliance on foreign-owned digital infrastructure.⁵⁵

A third recurring theme is the absence of robust multilateral design pathways. Many studies emphasize the need for global cooperation or shared standards, yet few explore the institutional mechanisms required to achieve them, such as how responsibilities should be allocated across

⁴⁹ Marcucci, Sara, et al. "Informing the Global Data Future: Benchmarking Data Governance Frameworks." *Data & Policy* 5 (January 2023). <https://doi.org/10.1017/dap.2023.24>.

⁵⁰ *Ibid.*

⁵¹ Kuzio, Jacqueline, et al., "Building Better Global Data Governance." *Data & Policy* 4 (2022): e24. <https://doi.org/10.1017/dap.2022.17>.

⁵² Taylor, *supra* note 43; Ishkhanyan, *supra* note 40; Roguski, *supra* note 42.

⁵³ OECD, 2022, *supra* note 46; Koutroumpis et al., *supra* note 48.

⁵⁴ United Nations Conference on Trade and Development (UNCTAD). *Data for Development*. Geneva: United Nations Conference on Trade and Development, 2024.

⁵⁵ Marcucci et al., *supra* note 49; Kwet, *supra* note 45.

governance levels, how compliance might be monitored, or how disputes could be resolved.⁵⁶ As a result, the literature often diagnoses fragmentation without proposing systems for coordination across divergent legal, political, and economic contexts.

Finally, the literature offers limited evidence on real-world outcomes. While conceptual and comparative analyses are abundant, evaluative research that examines how governance initiatives affect equity, interoperability, and development outcomes in practice is scarce. This lack of evaluative evidence is a significant barrier for policymakers seeking to design interventions that are both effective and contextually appropriate.

Collectively, these gaps highlight the importance of an approach that integrates normative principles, technical realities, and development-oriented priorities.

⁵⁶ Kuzio et al., *supra* note 51.

4. ANALYTICAL BRIEF: RETHINKING SOVEREIGNTY AND INTEROPERABILITY IN DATA GOVERNANCE

4.1 Introduction

With the advance of the internet and digital technologies, cross-border data flows have become foundational to economic and social functions, underpinning supply chains, digital payments, and public service delivery. At the same time, they generate governance challenges across multiple dimensions, including data privacy, security, economic value capture, and regulatory autonomy. As a result, data governance has evolved beyond the technical domain into a central policy issue concerning how data is accessed, controlled, and used across jurisdictions.⁵⁷ These challenges are particularly consequential in development contexts, where countries must balance participation in global data ecosystems with the need to manage risks, preserve policy space, and ensure that the benefits of data are equitably distributed.

In global data governance debates, “sovereignty” is often invoked in broad terms by both state and non-state actors to articulate claims over data itself as well as the infrastructure, algorithms, regulatory frameworks, and normative systems through which it is governed.⁵⁸ There has been a marked rise in the use of related concepts such as “data sovereignty”, “digital sovereignty”, and “AI sovereignty”, reflecting the growing importance of sovereignty in digital policy discourse. This trend is also reflected in broader public discourse, as shown in the sharp increase in searches of sovereignty-related terms on Google (see **Figure 1**).

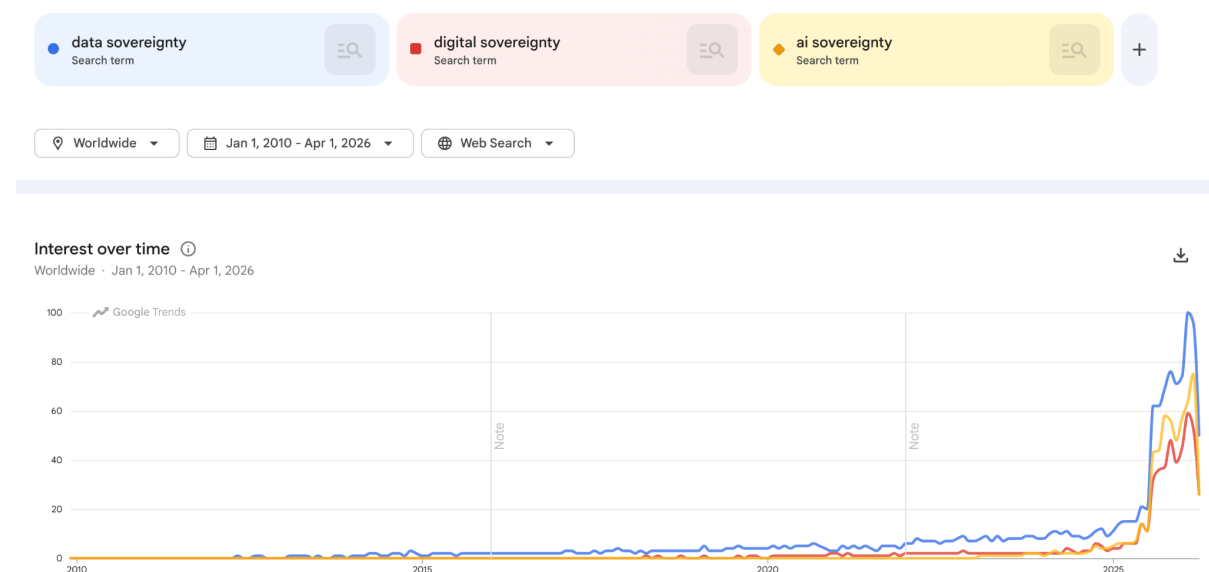


Figure 1: Relative search interest in sovereignty-related terms from 01/01/2010 to 01/04/2026 (Google Trends).

Values are indexed (0–100) and represent relative search interest over time. For interpretive purposes, the figure reflects overall trends and relative differences between terms rather than absolute values.⁵⁹

⁵⁷ Hassani, Hossein, Xu Huang, and Steve MacFeely. “Mapping the Evolution of Data Governance Scientific Research.” *Data & Policy* 7 (2025): e51. <https://doi.org/10.1017/dap.2025.10014>.

⁵⁸ Chander, Anupam and Haochen Sun. *Data Sovereignty: From the Digital Silk Road to the Return of the State*. Oxford: Oxford University Press, 2023.

⁵⁹ Google Trends, “Search interest for ‘data sovereignty,’ ‘digital sovereignty,’ and ‘AI sovereignty,’” accessed April 12, 2026, <https://trends.google.com>.

However, despite its widespread use, sovereignty is often invoked as an undifferentiated concept, limiting its analytical precision in guiding policy responses.⁶⁰ For state actors, sovereignty may encompass concerns related to security, regulatory autonomy, privacy, and capturing the economic value of data. For non-state actors, sovereignty may encompass claims to ownership, representation, or participation in decisions about how data regarding their communities is collected, stored, and used. These categories are not mutually exclusive and often overlap, reinforcing the complexity of sovereignty claims in practice.

One of the central and persistent tensions in global data governance lies in reconciling sovereignty concerns with cross-border data flows.⁶¹ While this tension is widely recognized, efforts to address it often remain circular, as policy responses are often premised on an assumed trade-off between sovereignty and openness. In practice, this framing can lead to defensive measures, such as broad data localization requirements or resistance to interoperability measures, that may mitigate certain risks while exacerbating others, including fragmentation and unequal participation in the global digital economy. As a result, the underlying drivers of these tensions remain unaddressed.

This analytical brief argues that the perceived tension between sovereignty and open data flows is often mischaracterized. It shows that this tension is better understood as a coordination problem arising from overlapping claims to authority over distinct underlying interests, rather than a trade-off between competing objectives. By disaggregating sovereignty claims in this way, the brief reframes interoperability not as a constraint on sovereignty, but as a set of governance mechanisms through which diverse actors can coordinate overlapping claims while enabling cross-border data flows, particularly in support of development objectives.

4.2 Sovereignty as Authority over Underlying Interests

4.2.1 Limitations of Territorial Sovereignty in the Digital Context

The principle of sovereignty is a hallmark of modern statehood in the post-Westphalian political and legal tradition.⁶² Under this formulation, a state exercises primary and exclusive authority over persons and things within its territory, and territorial intrusion is typically understood as the most direct challenge to state authority.⁶³

Cyberspace, however, is not composed of digital equivalents of states and their borders. Given the a-territorial nature of data flows, threats to state authority in the digital age can arise without any physical territorial intrusion.⁶⁴ As a result, the core elements of traditional sovereignty—absolute authority, exclusivity, and territoriality—do not map neatly onto the digital domain. This creates a fundamental governance challenge as states seek to exercise authority over data and digital systems that are inherently transnational and distributed. As cyberspace has become a central arena of

⁶⁰ Felix von Scherenberg, Moritz Hellmeier, and Boris Otto, "Data Sovereignty in Information Systems," *Electronic Markets* 34, no. 1 (2024): 15, <https://doi.org/10.1007/s12525-024-00693-4>.

⁶¹ Hummel, Patrik, Matthias Braun, Max Tretter, and Peter Dabrock. "Data sovereignty: A review." *Big Data & Society* 8, no. 1 (2021): 2053951720982012, <https://doi.org/10.1177/2053951720982012>.

⁶² Nagan, Winston P., and Aitza M. Haddad. "Sovereignty in theory and practice." *San Diego Int'l LJ* 13 (2011): 429.

⁶³ Gray, John. *Al Qaeda and What It Means to Be Modern*. New York: The New Press, 2003.

⁶⁴ Daskal, Jennifer. "The un-territoriality of data." *Yale LJ* 125 (2015): 326.

national policy, global governance, and development, clarifying what ‘sovereignty’ means in this context is essential for shaping development outcomes.⁶⁵

Much of the existing literature on digital and data sovereignty,⁶⁶ including recent work on AI sovereignty, treats sovereignty as a fixed attribute of states or conceptualizes it as control over different layers of the digital stack, such as infrastructure, algorithms, and data.⁶⁷ Other strands emphasize the policy objectives associated with sovereignty claims, including economic development, national security, and strategic autonomy.⁶⁸ While these approaches recognize the composite nature of sovereignty debates, they tend to focus on domains of control or stated policy objectives, rather than on the underlying interests over which authority is being asserted. As a result, they provide limited insight into how and why sovereignty claims are mobilized in practice, why different actors invoke sovereignty in specific contexts, and more importantly, how these claims can translate into concrete governance responses.

This analytical brief reconceptualizes sovereignty as claims to authority over underlying interests, providing a more contextualized understanding of how sovereignty concerns shape data governance debates. Given the a-territorial nature of data flows, authority cannot be understood solely in territorial terms. Rather, sovereignty claims reflect efforts by different actors to assert authority over specific interests, depending on the context and their strategic objectives. Under this formulation, sovereignty is better understood not as authority exercised within a bounded territory, but as authority asserted over a sphere of interests.

This conceptual reframing allows the relationship between sovereignty and cross-border data flows to be understood as a coordination problem arising from overlapping claims to authority, rather than as a trade-off. Interoperability can then be understood as a set of governance mechanisms through which these claims can be coordinated in practice. While such mechanisms can mitigate tensions and enable cooperation, their effectiveness ultimately depends on how underlying interests are prioritized and how power and institutional capacity are distributed across actors.

4.2.2 Sovereignty as Claims over Underlying Interests

A review of submissions by members, observers, and other stakeholders to the UN CSTD Multi-Stakeholder Working Group on Data Governance suggests that sovereignty claims can be disaggregated into several broad categories of underlying interests. These categories are derived

⁶⁵ Brooke Tanner et al., *Is AI Sovereignty Possible? Balancing Autonomy and Interdependence* (Washington, DC: Brookings Institution, February 2026), https://www.brookings.edu/wp-content/uploads/2026/02/20260217_AI_sovereignty_final.pdf.

⁶⁶ See, *Ibid* and Sean Mullin and Jaxson Khan, *Sovereignty by Design: Strategic Options for Canadian AI Sovereignty* (Toronto: Munk School of Global Affairs and Public Policy, 2026), <https://aicompetitiveness.ca/assets/Sovereign-by-Design-Full-Report-2026.pdf>; Adam Clark, *Research Briefing - Digital Sovereignty* (London, UK: House of Commons Library, 2026), <https://researchbriefings.files.parliament.uk/documents/CBP-10547/CBP-10547.pdf>.

⁶⁷ Roguski, Piotr. “Layered Sovereignty: Adjusting Traditional Notions of Sovereignty to a Digital Environment.” In 11th International Conference on Cyber Conflict: CyCon, edited by Tomáš Minárik, et al., 347–359. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2019.

⁶⁸ See, Data Sovereignty: From the Digital Silk Road to the Return of the State, *supra* note 58 and Hummel, Patrik, Matthias Braun, Max Tretter, and Peter Dabrock, *supra* note 61.

inductively from recurring themes across submissions and reflect how different actors articulate sovereignty concerns in practice.⁶⁹

1. **Security Interests:** invoking sovereignty to assert authority over critical data and digital infrastructure in order to safeguard national security and protect against external risks. This includes efforts to control the full lifecycle of data, strengthen domestic oversight of critical digital infrastructure, and limit exposure to foreign access or interference. Common measures include data localization or transfer restrictions, the development of sovereign or government-controlled infrastructure, and the implementation of data classification and security regimes. Such measures are commonly justified as necessary to preserve state capacity and reduce strategic dependence, particularly in contexts where external control over data infrastructure is perceived as a source of vulnerability.⁷⁰
2. **Economic Interests:** invoking sovereignty to assert control over data as an economic resource and to shape how value is generated, captured, and distributed in the global digital economy. This includes efforts to retain greater value from domestically generated data, address structural asymmetries in global data value chains, and support data-driven development strategies. Common approaches include framing data as a sovereign economic resource or core factor of production, regulating cross-border data flows and processing to avoid extractive dynamics (such as the “raw data trap”), and using fiscal and regulatory tools to capture value from digital activities, including platform-based economies (e.g., digital services taxes).⁷¹
3. **Regulatory Interests:** invoking sovereignty to preserve regulatory autonomy and maintain the “policy space” necessary to govern digital systems in line with domestic legal, institutional, and development priorities. This includes efforts to retain authority over the design, interpretation, and enforcement of rules governing data and digital systems, and to ensure that such rules reflect domestic contexts rather than externally imposed governance models. Common expressions include resisting uniform or externally driven regulatory frameworks, delimiting the scope of international rulemaking processes including trade agreement frameworks that may constrain domestic policymaking, and opposing the extraterritorial application of foreign laws that extend jurisdiction over domestic data and entities.⁷²
4. **Community and Social Interests:** invoking sovereignty as a claim to authority over data to protect collective well-being, cultural integrity, and ethical agency, shifting the focus from state-centric control toward social justice and self-determination. This includes efforts to recognize collective rights over data, ensure meaningful participation in decisions about its use, and prevent forms of data extraction that undermine community autonomy or cultural identity. Common expressions include asserting community-based governance over data (particularly for

⁶⁹ The submissions referenced in this section are illustrative of the different sovereignty-based claims identified across submissions to the Working Group. They are not exhaustive, do not imply endorsement, and should be interpreted in the context of the full submissions.

⁷⁰ Submissions from Africa Rights Network (e.g. “smart location practices” where “Sovereign Data” concerning identity and security remain local, while other development data concerning climate, health, and trade, is permitted to flow freely within regional blocks), Anita Gurumurthy (IT for Change), Brazil (e.g. Serpro and Dataprev), Cuba, Gambia (G-cloud policy), Iran, World Digital Technology Academy.

⁷¹ Submission from Anita Gurumurthy (IT For Change), Brazil, China, Cuba.

⁷² Submissions from Anita Gurumurthy (IT for Change), Brazil, Cuba, Derechos Digitales, Gambia, Iran, Rethink Trade.

Indigenous Peoples), restricting the unauthorized use of cultural data and traditional knowledge, and framing data as a collective or public resource to support equitable development outcomes. These claims also extend to addressing data-related inequalities, including issues of representation, bias, and marginalization of certain communities within digital systems.⁷³

5. **Strategic Interests:** invoking sovereignty to shape long-term development trajectories, build domestic capacities, and position actors within the global digital economy. Unlike security interests, which focus on immediate risks, strategic claims are forward-looking and concerned with reducing structural dependencies, avoiding technological lock-in, and maintaining decision-making autonomy over time. This includes efforts to develop domestic and regional digital infrastructure (such as data centers, cloud systems, and digital public infrastructure), strengthen participation in global data value chains, and retain critical capabilities, including talent and innovation capacity. Strategic claims also extend to influencing the global digital order, including asserting voices in international fora and shaping norms and standards in ways that reflect domestic and regional priorities.⁷⁴

Taken together, these categories illustrate that sovereignty claims in data governance reflect distinct but overlapping efforts to assert authority over security, economic, regulatory, social, and strategic interests, reinforcing the need for governance approaches capable of coordinating these claims in practice.

4.2.3 Analytical Implications

Under this formulation, actors invoke sovereignty to assert authority over distinct underlying interests, reflecting their strategic priorities, stage of development, and technological capabilities. Functionally, this shifts sovereignty from a territorially bounded concept to a relational one, defined by how authority is asserted across overlapping and a-territorial domains of interests.

This revised typology provides three analytical insights:

1. Clarifying how and why sovereignty is invoked across different actors and contexts, by linking claims to specific underlying interests;
2. Revealing how multiple actors may assert overlapping and, at times, competing sovereignty claims over the same data asset, infrastructure, or digital system; and
3. Showing how individual sovereignty claims may simultaneously advance multiple underlying interests, giving them a layered and multifunctional character.

Together, these insights highlight the plural, overlapping, and contested nature of authority in the digital domain. By reframing sovereignty in this way, the framework shifts the analytical focus from balancing sovereignty against openness to coordinating overlapping claims to authority. This in turn allows for more targeted and context-specific governance responses, particularly in ways that support development objectives while preserving policy space.

⁷³ Submissions from Sarawak Multimedia Authority, Indigenous Data Network, Humanistic Buddhism Centre, Iran.

⁷⁴ Submission from EU, Hungary, Tech Global Institute, Apesoft Peru, Brazil; Gambia, Canada, Tech Global Institute and Indigenous stakeholders.

Importantly, while sovereignty is often invoked to protect legitimate underlying interests, it is not a neutral concept. Such claims may be strategically deployed to justify restrictive policies, consolidate control, or advance geopolitical objectives, and are frequently advanced and contested in asymmetrical contexts, where differences in economic, technological, and institutional power shape whose claims prevail in practice. Recent policy debates illustrate how these dynamics can limit openness, reduce competition, or undermine international cooperation, particularly where actors have the power to project regulatory or market influence across borders.⁷⁵ Recognizing this dual character underscores the need for governance approaches, such as interoperability, that can both respect sovereignty and mitigate its potentially fragmenting effects.

4.3 Interoperability as a Governance Mechanism for Coordinating Sovereignty Claims

4.3.1 From Trade-off to Coordination: Rethinking the Sovereignty ↔ Interoperability Tension

Sovereignty and interoperability are often framed as competing paradigms, representing one of the core structural tensions in global data governance, particularly in the context of development. This tension reflects a techno-political challenge, rather than a purely technical issue of systems integration.⁷⁶ In practice, it manifests in several recurring ways:

- Interoperability is often perceived as a proxy for unrestricted data flows, raising concerns that technical standardization, without appropriate governance safeguards, could constrain a state's ability to regulate its data assets effectively;⁷⁷
- Security-driven responses, such as data localization requirements, have emerged as default mechanisms to address perceived loss of control once data leaves domestic jurisdiction;⁷⁸
- Legal interoperability is often viewed with caution due to concerns that it may lead to a “race to the bottom” or the *de facto* diffusion of governance standards that do not reflect domestic values, institutional capacities, and development priorities;⁷⁹ and
- Conversely, prioritizing sovereignty is frequently perceived as constraining participation in the global digital value chain, with potential dampening effects on innovation and competitiveness.⁸⁰

Taken together, these concerns reinforce the perception of an inherent trade-off between asserting sovereignty over data and digital systems and enabling cross-border data flows. Addressing this tension is particularly important for actors, including developing countries, that must balance participation in global data ecosystems with the need to retain policy space and build governance capacity.

As previously highlighted, sovereignty, as invoked in global data governance debates, is more precisely understood as a set of overlapping claims to authority over distinct underlying interests

⁷⁵ James Gorgen, “How Trump’s Data Regulation Crackdown Undermines Digital Sovereignty,” Tech Policy Press, March 12, 2026, <https://www.techpolicy.press/how-trumps-data-regulation-crackdown-undermines-digital-sovereignty/>.

⁷⁶ González Morales, Luis Gerardo, and Tom Orrell. “Data interoperability: A practitioner’s guide to joining up data in the development sector.” (2018), <https://unstats.un.org/wiki/spaces/InteropGuide/pages/36143964/Home>.

⁷⁷ Submission from Anita Gurumurthy (IT for Change).

⁷⁸ Submission from Talla Ndiaye (Digital Impact Alliance).

⁷⁹ Submission from Derechos Digitales, Research ICT Africa, Tech Global Institute.

⁸⁰ Submission from Timea Suto (International Chamber of Commerce).

rather than as a singular and indivisible construct. Under this framework, the apparent tension between sovereignty and interoperability is better characterized as a coordination problem arising from overlapping claims to authority, rather than a binary trade-off. This reframing shifts the analytical focus from balancing competing objectives to structuring how authority is coordinated across an interdependent data ecosystem.

Interoperability, in this context, is best understood as a set of governance mechanisms that facilitate the coordination of overlapping claims to authority across diverse legal, institutional, and normative frameworks. It enables cross-border data flows while advancing and protecting the underlying interests articulated through sovereignty claims.

While there is growing convergence around the importance of interoperability, existing contributions have primarily focused on its institutional and policy dimensions. This analysis builds on these insights by operationalizing interoperability as a coordination mechanism, examining how it mediates overlapping sovereignty claims and shapes their interaction in practice.

4.3.2 Operationalizing Interoperability: An Illustrative Example

To illustrate how interoperability operates as a coordination mechanism, consider a stylized example in which a foreign digital platform provider offers its services within a domestic market. This example isolates key actors, their respective claims to authority, and the underlying interests those claims are intended to advance, as summarized in the table below.

	Foreign Digital Platform Provider	Local Users and Communities	State
Sovereignty Claim	Platform-level control over data access, processing, storage, and monetization.	Authority over personal and collective data (access, consent, protection).	Regulatory authority over data flows and platform operations within jurisdiction.
Key Underlying Interests	Economic: value capture from data and services. Strategic: ecosystem control and sustained data access. Regulatory: operational flexibility and limited constraints.	Social: privacy, dignity, and control over data use. Economic: preventing exploitation and unequal value extraction.	Regulatory: policy space and governance authority Security: protection from external access and interference Strategic: domestic capability-building and reduced dependency

The example highlights how different actors invoke sovereignty claims to advance distinct underlying interests. While these claims are not inherently mutually exclusive, they can generate tensions in practice, particularly where interests related to data control, value capture, and regulatory authority intersect. In the absence of coordination, such tensions may lead to fragmentation—through restrictive measures such as data localization—or to concentration of control within dominant platforms. Interoperability, in this context, provides mechanisms for coordinating these overlapping

claims to authority in a way that supports cross-border data flows while supporting value distribution, and the ability of actors to pursue their respective governance objectives.

There is growing convergence that interoperability extends beyond technical compatibility and operates across multiple layers. Existing frameworks typically distinguish between technical, semantic, organizational, and legal dimensions. Building on this foundation, the analysis adopts a more governance-oriented approach, focusing on how the different layers of interoperability coordinate overlapping sovereignty claims in practice.

For purposes of this brief, the following layers are particularly relevant:⁸¹

- **Technical Interoperability** enables systems to exchange data through shared standards and protocols;
- **Normative Interoperability (including semantic interoperability)** ensures that data can be consistently interpreted and used across contexts, including shared definitions, principles, and expectations;
- **Institutional Interoperability (as an extension of organizational interoperability)** coordinates processes, roles, oversight and governance arrangements across organizations; and
- **Legal Interoperability** enables data and digital transactions to be recognized, transferred, and relied upon across jurisdictions.

Building on this multi-layered understanding of interoperability, the table below illustrates how different layers engage and coordinate the underlying interests advanced by different actors in the illustrative example.

	Foreign Digital Platform Provider	Local Users and Communities	State
Sovereignty Claim	Platform-level control over data access, processing, storage, and monetization.	Authority over personal and collective data (access, consent, protection).	Regulatory authority over data flows and platform operations within jurisdiction.
Key Underlying Interests	Economic: value capture from data and services. Strategic: ecosystem control and sustained access to data. Regulatory: operational flexibility and limited constraints.	Social: privacy, dignity, and control over data use. Economic: preventing exploitation and unequal value extraction.	Regulatory: policy space and governance authority. Security: protection from external access and interference. Strategic: domestic capability-building and reduced dependency.
Technical Interoperability <i>Coordination through systems design</i> (Examples: federated data systems, interoperable digital identity, privacy-enhancing technologies)	• Maintains access to distributed data without full centralization • Supports scalable service delivery • Limits ability to fully lock in data ecosystems	• Keeps data in trusted/local environments • Reduces risks of unauthorized access and aggregation • Supports more equitable participation in data use	• Maintains oversight of data storage and processing • Reduces reliance on foreign infrastructure • Supports sovereignty without full data isolation
Normative Interoperability <i>Coordination through shared meanings and norms</i> (Examples: shared data governance principles, ethical standards for AI and data use, trust frameworks, codes of conduct)	• Builds user trust and legitimacy • Introduces reputational accountability • Constrains certain business practices	• Strengthens confidence in data use • Promotes fairness and ethical safeguards • Enables trust-based participation	• Enhances legitimacy of governance frameworks • Supports alignment with international norms and standards
Institutional Interoperability <i>Coordination through governance</i> (Examples: data-sharing agreements, joint governance bodies, coordinated enforcement mechanisms)	• Reduces regulatory uncertainty across jurisdictions • Enables coordinated oversight and enforcement • May increase compliance costs	• Strengthens oversight and protection mechanisms • Improves consistency of enforcement • Enhances accountability across systems	• Expands capacity to govern cross-border flows • Enables cooperation and joint enforcement • Helps address institutional constraints
Legal Interoperability <i>Coordination through recognition across jurisdictions</i> (Examples: mutual recognition frameworks, adequacy decisions, cross-border transfer mechanisms)	• Enhances predictability across jurisdictions • Supports scalability of operations • Introduces compliance obligations and potential rigidity	• Strengthens protections against exploitative practices • Reduces regulatory gaps and uneven safeguards	• Preserves regulatory autonomy through conditional transfers • Enables recognition of equivalent regimes • Avoids full harmonization

The table above illustrates how different layers of interoperability coordinate the interaction of competing sovereignty claims across actors. As each layer engages different underlying interests,

⁸¹ *Interoperability of Data Governance Regimes: Challenges for Digital Trade Policy*, Bacchus J, Borchert I, Marita-Jaeger M, Ruiz Diaz J, 2024, <https://citp.ac.uk/publications/interoperability-of-data-governance-regimes-challenges-for-digital-trade-policy>

outcomes depend on how specific mechanisms are designed and combined in practice. Taken together, these layers structure how sovereignty claims coexist, enabling cross-border data flows while preserving space for actors to advance their respective interests, including development objectives.

Importantly, the governance outcomes are contingent on several interrelated factors, including: (i) **design choices**, such as whether interoperability mechanisms prioritize openness, control, or hybrid arrangements; (ii) **institutional capacity**, particularly the ability of states—especially in developing contexts—to implement and enforce interoperable systems effectively; and (iii) **power dynamics**, including asymmetries between states, platform providers, and other stakeholders that shape whose interests are prioritized and how interoperability mechanisms are implemented in practice.

Within these constraints, interoperability remains central to data governance, as absolute or fully insulated forms of sovereignty are neither attainable nor desirable in an interconnected digital ecosystem. Interoperability provides the institutional and technical means to manage these trade-offs, enabling multiple actors to exercise authority simultaneously within shared data environments. These dynamics are particularly salient in a development context, where differences in capacity and bargaining power shape whether interoperability frameworks enable meaningful participation or reproduce existing inequalities.

4.4 Policy Implications

Unlocking the apparent tension between sovereignty and interoperability by reframing sovereignty into constituent underlying claims and examining how interoperability mechanisms can coordinate those claims inform policymaking as follows:

- Data governance debates should move beyond broad and abstract invocations of sovereignty toward identifying the specific underlying interests that actors seek to protect. Disaggregating sovereignty claims into their constituent interests enables more targeted and context-specific policy responses, facilitates coalition-building among actors with shared interests, and reduces the risk that broad, restrictive measures exacerbate fragmentation or reinforce existing inequalities, particularly for developing countries with more limited policy space.
- Interoperability should not be framed as a trade-off against sovereignty. Rather, it should be understood as a set of enabling governance mechanisms through which sovereignty claims can be coordinated without resorting to excessive protectionism or unrestricted openness. This reframing allows policymakers to move beyond binary choices and design systems that support both cross-border data flows and the exercise of legitimate authority claims.
- The effectiveness of interoperability depends not only on the choice of mechanisms, but on how they are designed, combined, and sequenced in practice. Different layers of interoperability—technical, normative, institutional, and legal—affect different interests and actors in distinct ways. Policymakers should adopt a layered and context-specific approach, calibrating mechanisms to balance relevant interests rather than applying uniform one-size-fits-all solutions.

- The analytical framework developed in this brief can be applied beyond cross-border data flows to adjacent domains, including AI governance and digital infrastructure policy across national, regional, and international levels. By systematically identifying underlying interests and mapping how interoperability mechanisms shape their interaction, policymakers can better navigate emerging governance challenges across the digital ecosystem.

4.5 Looking Ahead

As data governance debates evolve, particularly in AI governance, sovereignty claims will remain central. They resonate politically because they signal that important interests are at stake, even when those interests are not clearly articulated. Policymakers and practitioners need not take such claims at face value. Instead, they can interpret them more analytically by identifying the underlying interests being advanced.

This brief has proposed a framework for doing so. By reconceptualizing sovereignty as claims to authority over distinct underlying interests, it shifts the focus from abstract debates toward how competing interests can be coordinated in practice. Within this framing, interoperability is not a solution that eliminates sovereignty tensions, but a set of governance mechanisms through which they can be managed, negotiated, and, where possible, aligned. Such coordination, however, does not occur in a neutral environment. Outcomes depend on how mechanisms are designed, which interests are prioritized, and the relative power of the actors advancing them.

This also implies that pursuing “full” or self-contained sovereignty is neither realistic nor necessarily desirable. Authority over data and digital systems is exercised across multiple layers, each involving different capabilities, dependencies, and trade-offs. Sovereignty is therefore not a singular end state, but an incremental process of managing dependencies and building leverage. The key policy question is not how to eliminate dependency altogether, but to identify which dependencies are acceptable, which capabilities are most critical to develop, and how these choices shape a country’s ability to exercise agency over time.

Ultimately, interoperability does not resolve the political and structural tensions embedded in data governance. It provides a means of managing them under conditions of interdependence. Whether it enables more inclusive and development-oriented outcomes will depend on how these mechanisms are designed, who participates in shaping them, and how asymmetries in capacity and power are addressed.

The central challenge for global data governance, then, is not to eliminate sovereignty claims, but to actively shape how they are coordinated under conditions of interdependence and asymmetry in ways that support more equitable and development-oriented outcomes.

5. THEMATIC ARTICLES

5.1 From Policy to Public, from Public to Policy: Making Data Governance Legible in the Digital Age

5.1.1 Introduction: The Stakes of Data Governance

Data nowadays permeates every aspect of life. It shapes who accesses credit, healthcare, education, and employment; it determines the terms on which individuals, communities, and states participate in global markets; and it increasingly mediates the relationship between citizens and public institutions. The governance of data, namely the rules, norms, and institutions that determine how data is collected, stored, shared, and monetised, is therefore not a technical matter, but rather a profoundly political one. Political, here, in the deepest sense of the word: pertaining to all that concerns those who live in the *polis*, that is, citizens and their life in common.

Nevertheless, the distribution of benefits and harms from data is deeply unequal. At the individual level, people routinely surrender data under conditions they do not understand, in exchange for services whose terms they cannot meaningfully negotiate. At the collective level, instead, as the UNCTAD Digital Economy Report of 2021 documents, a small number of platform corporations, concentrated in the United States and China, capture a disproportionate share of the value generated by global data flows, while the countries and communities that produce much of that data, particularly in the Global South, receive little in return.⁸²

The consequences of this are not only economic. Data governance failures enable the surveillance of political dissidents, the algorithmic profiling of ethnic and religious minorities, the manipulation of electoral processes, and the erosion of the conditions under which democratic deliberation is possible. They determine whether public health systems can access the data they need to respond to crises, or whether that data remains locked within proprietary platforms. They shape whether artificial intelligence systems amplify or correct existing patterns of discrimination.

Against this backdrop, the institutions and frameworks through which data governance is negotiated - including the UNCTAD CSTD Working Group on Data Governance - are not peripheral bureaucratic exercises. They are sites where fundamental questions of economic justice and political power are being decided. The public has a direct stake in how those questions are answered, whether or not it currently knows it. And that gap, between the stakes of data governance and the degree to which those stakes are publicly understood, is precisely the problem this article sets out to address.

5.1.2 The recognition gap: why data governance lacks public salience?

A 2023 Pew Research Center survey found that 67 per cent of American adults understand little or nothing about what companies do with their personal data, a figure that has risen since 2019 despite increased regulatory activity. The share of Americans who feel they do not understand data privacy

⁸² UNCTAD, *Digital Economy Report: Cross-border data flows and development: For whom the data flow*, (2021), 16-17; 107. Available here: https://unctad.org/system/files/official-document/der2021_en.pdf

laws now stands at 72 per cent.⁸³ In Europe, even after the General Data Protection Regulation (GDPR)'s high-profile rollout in 2018, only 22 per cent of internet users report feeling adequately informed about how their data is used. Rughinis and colleagues (2021), analysing Eurobarometer data across twenty-eight EU countries, find that only one of four distinct clusters of digital citizens, the “data citizens”, comprising 29 per cent of the population, has substantive understanding of the regulatory framework governing their data.⁸⁴

This is what we might call the recognition gap: the distance between the actual significance of data governance and the degree to which that significance is acknowledged in public and political life. As already stressed, the risk is that data governance is something debated among lawyers, technologists, and trade negotiators, but rarely figures in electoral platforms, street-level mobilisation, or sustained media attention of the kind that has driven action on, for instance, climate change or financial regulation.

This gap is not accidental. It can be attributed to several structural factors, three of which are summarized in this article. The first is the invisibility of harm. Unlike environmental degradation or labour exploitation, the harms produced by poor data governance tend to be opaque, individualised, and difficult to attribute to a specific cause. There is rarely a visible disaster, an identifiable victim, or a clear perpetrator. Zuboff (2019) has argued that this invisibility is in part a deliberate feature of surveillance capitalism: the extraction of behavioural data depends on users not fully understanding what is happening to them or why it matters.

The second factor is the fragmentation of language. Data governance is, in practice, discussed under many different labels: privacy, cybersecurity, digital rights, AI ethics, data sovereignty and interoperability, platform regulation. Each of these captures part of the problem but none of which covers it whole. This fragmentation is not merely terminological. As Dencik et al. (2019) argue in their foundational work on data justice, the proliferation of disconnected frames prevents the emergence of the cross-sectoral coalitions that political mobilisation requires. When privacy advocates, development economists, indigenous rights movements, and labour organisers are all addressing aspects of the same structural problem without a shared vocabulary, their collective voice is weakened.

The third factor is the technocratic character of existing governance discourse. The dominant institutional language of data governance, drawn from trade law, technical standards, and regulatory frameworks, is inaccessible to most citizens and to many civil society actors. This is not simply a matter of complexity: it reflects a deeper assumption, embedded in how these conversations have been structured: that data governance is a problem for experts rather than a matter of public concern. The result is a self-reinforcing dynamic in which the absence of accessible language produces a lack of public engagement, which in turn reduces the political pressure to invest in accessible communication.

⁸³ McClain, Coleen, Faverio Michelle, Anderson Monica, Park Eugenie, “How Americans View Data Privacy”, *Pew Research Center*, October 18, 2023. Accessed April 7, 2026 https://www.pewresearch.org/wp-content/uploads/sites/20/2023/10/PI_2023.10.18_Data-Privacy_FINAL.pdf?_gl=1*8yonnq*_up*MQ..*_gs*MQ..&gclid=CjwKCAjwnN3OBhA8EiwAfpTYegGMM6k0_inOn5I5U5W_9d7AugYVrdpIXHT9rprSD2Mn419vg8OXjhoCW4oQAvD_BwE&gbraid=0AAAAA-ddO9F7BTTNtcH5TwHdgl8Kq5ziO

⁸⁴ Rughinis, C., Rughinis, R., Toma, S. and Vulpe, S.N. (2021). “From Social Netizens to Data Citizens: Variations of GDPR Awareness in 28 European Countries.” *Computers Law & Security Review* 42(2021), <https://doi.org/10.1016/j.clsr.2021.105585>

5.1.3 Communication theory as a diagnostic and prescriptive tool

The challenge of making an abstract, structurally complex issue legible to public audiences is not unique to data governance. Communication scholarship offers a well-developed set of tools for understanding why some issues achieve public salience while others do not, and for thinking about how salience can be deliberately cultivated.

Agenda-setting theory, first articulated by McCombs and Shaw (1972) in their landmark study of the 1968 US presidential election, established that media coverage does not simply reflect public concern, it actively constitutes it.⁸⁵ Issues that receive sustained, prominent coverage acquire public salience; issues that do not, however important, remain invisible to most people. The implications for data governance are direct: without a concerted effort to insert the issue into mainstream media and political agendas, not as a technical story, but as a story about power, rights, and justice, it will continue to occupy the margins of public attention.

Issue framing theory, developed by Entman (1993) and others, adds a further layer of analysis.⁸⁶ How an issue is framed, what aspects are emphasised, what values it is connected to, who is identified as responsible, determines not only whether people pay attention, but how they respond. The same policy can generate very different political reactions depending on whether it is framed as a technical regulatory question, an economic opportunity, or a matter of fundamental rights. Nisbet (2009), writing specifically about climate change communication, has shown that the shift from a scientific frame to a justice and equity frame was crucial in broadening the climate movement beyond specialist audiences and connecting it to existing political identities and mobilisation structures.⁸⁷

The experience of climate communication offers the most instructive - if imperfect - analogy for data governance. In the 1980s and early 1990s, climate change was widely perceived as a problem for scientists and government planners, not for citizens.⁸⁸ The transformation that followed was not purely the product of worsening conditions or stronger science: it was also the product of deliberate investment in narrative infrastructure. The Intergovernmental Panel on Climate Change (IPCC)'s Summary for Policymakers established a model for translating technical consensus into accessible, politically actionable language. Civil society organisations developed campaigns that personalised abstract risks through concrete stories and images. And a set of bridging concepts such as “the carbon footprint”, “net zero”, “the climate emergency” gave publics and journalists shared reference points around which coverage and debate could come together.

⁸⁵ McCombs, Maxwell E., and Donald L. Shaw. “The Agenda-Setting Function of Mass Media.” *The Public Opinion Quarterly* 36, no. 2 (1972): 176–87. <http://www.jstor.org/stable/2747787>.

⁸⁶ Entman, R. M. (1993). “Framing: Toward clarification of a fractured paradigm”. *Journal of Communication* 43, no. 4 (1993), 51–58. <https://doi.org/10.1111/j.1460-2466.1993.tb01304.x>

⁸⁷ Nisbet, Matthew C., “Communicating Climate Change: Why Frames Matter for Public Engagement”, *Environment: Science and Policy for Sustainable Development* 51, no. 2(2009): 12-23, <https://doi.org/10.3200/ENV51.2.12-23>

⁸⁸ See Capstick, Stuart, Lorraine Whitmarsh, Wouter Poortinga, Nick Pidgeon, and Paul Upham. 2014. “International Trends in Public Perceptions of Climate Change over the Past Quarter Century.” *Wiley Interdisciplinary Reviews: Climate Change* 6 no. 1 (2014): 35–61. <https://doi.org/10.1002/wcc.321>; and Nisbet, Matthew C., and Teresa Myers. “Trends: Twenty Years of Public Opinion about Global Warming.” *The Public Opinion Quarterly* 71, no. 3(2007): 444–70. <https://www.jstor.org/stable/4500386>; and

Data governance lacks equivalent infrastructure. There is no agreed “data footprint”, no widely shared image of what data extraction looks like, no mobilising slogan that connects the issue to everyday experience. The concept of “data justice”, as developed by Dencik et al. (2019)⁸⁹ and further elaborated by Milan and Treré (2019)⁹⁰ in their work on data governance from the Global South, has the potential to serve as such a bridging concept connecting individual experience of digital harm to structural questions of power and distribution, but it has not yet achieved the kind of institutional uptake or public resonance that would give it agenda-setting force.

5.1.4 Recommendations: building narrative infrastructure for data governance

Addressing the recognition gap requires deliberate, sustained investment in what we might call narrative infrastructure: the shared language, institutional practices, and communication strategies that make it possible for a complex issue to enter and remain on public agendas and ultimately drive policy change.⁹¹ Here are proposed five concrete directions.

1. First, international institutions, and the CSTD Working Group on Data Governance in particular, should work toward a shared minimum lexicon for data governance communication. This does not mean imposing terminological uniformity on a diverse field, but identifying a small set of concepts that are both analytically precise and publicly accessible, and using them consistently across documents, communications, and public engagements. Concepts such as data justice, data sovereignty, and digital commons have the potential to serve this function, provided they are deployed with deliberate attention to their communicative as well as technical dimensions. Gurumurthy and Chami (2019) have argued that such a lexicon is a precondition for meaningful participation by civil society actors, particularly in the Global South, in governance conversations that currently exclude them by design.⁹²
2. Second, multilateral institutions should adopt a systematic practice of translating technical governance documents into accessible public-facing versions modelled explicitly on the IPCC's approach. Every major output of a data governance working group or intergovernmental process should be accompanied by a plain-language summary, developed with the involvement of communication specialists and civil society organisations, that situates the technical content within a recognisable narrative of rights, justice, and collective interest.
3. Third, multilateral institutions should complement the above mentioned institutional translation by introducing an additional communication layer that effectively reaches broader publics. A critical limitation of even the most accessible policy documents is their

⁸⁹ Dencik, Lina, Arne Hintz, Joanna Redden, and Emiliano Treré. 2019. “Exploring Data Justice: Conceptions, Applications and Directions.” *Information, Communication & Society* 22, no. 7(2019): 873–81, <https://doi.org/10.1080/1369118X.2019.1606268>

⁹⁰ Milan, Stefania, & Treré Emiliano, “Big Data from the South(s): Beyond Data Universalism”. *Television & New Media* 20, no. 4(2019), 319–335. <https://doi.org/10.1177/1527476419837739>

⁹¹ See, Blum, Sonja, and Johanna Kuhlmann. 2019. “Stories of How to Give or Take – towards a Typology of Social Policy Reform Narratives.” *Policy and Society* 38 (3): 339–55. <https://doi.org/10.1080/14494035.2019.1657607> and McBeth MK, Jones MD and Shanahan EA, “The narrative policy framework”, in (2018). *Theories of the Policy Process*, ed. M. Weible, C., & Sabatier, P.A. (Routledge, 2018) <https://doi.org/10.4324/9780429494284>

⁹² Alemany, Cecilia, Gurumurthy Anita, Chami Nandini, “Gender Equality in the Digital Economy: Emerging Issues,” *Feminist Digital Justice* 1(2019). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3872572

discoverability: they reach those already looking, not the broader publics that data governance needs to mobilise.⁹³ Bridging this gap requires an additional layer of intermediaries — science communicators, journalists, and digital creators capable of translating governance concepts into formats that circulate in mainstream media environments.⁹⁴ The climate movement has demonstrated the power of this model, from the IPCC scientist who becomes a trusted public voice to the social media creator who makes carbon budgets legible to millions. Cultivating equivalent intermediaries for data governance, and creating institutional incentives, such as recognition schemes or dedicated funding, for academics and practitioners willing to invest in public communication, should be treated not as a secondary concern but as a structural component of any serious governance communication strategy.

4. Fourth, researchers and advocates working on data governance should actively build coalitions with movements that are already addressing its consequences without necessarily naming the underlying issue. Indigenous rights organisations confronting the use of community data without consent, labour movements resisting algorithmic management, and environmental justice groups concerned with data-driven surveillance of activists are all, in different registers, engaged with problems that data governance frameworks are designed to address. A deliberate strategy of frame alignment, identifying shared values and connecting separate struggles through a common language, is likely to be more effective in building public salience than any amount of technical advocacy conducted within existing silos.
5. Fifth, and perhaps most importantly, the field needs cases: concrete, narratable, human-scale stories that make the consequences of data governance visible and attributable. As the growing body of work of the Narrative Policy Frameworks (NPF) illustrates, policy moves after stories, not before them.⁹⁵ This means not only surfacing failures, but amplifying instances where good governance has produced tangible benefits. The Cambridge Analytica scandal⁹⁶ crystallised an abstract problem into a form that publics and legislators could grasp; what data governance needs is a sustained effort to surface such “focusing events” across multiple contexts, balanced by stories of what becomes possible when data is governed well.⁹⁷ Disaster response offers some of the most compelling positive examples. Following the 2010 Haiti earthquake, the rapid aggregation of mobile network data by telecommunications providers, shared under emergency data-sharing agreements with humanitarian organisations, enabled responders to map population displacement in near real time and direct aid to areas that would otherwise have remained invisible to relief

⁹³ See Nisbet, Matthew C., and Dietram A. Scheufele. “What’s Next for Science Communication? Promising Directions and lingering distractions” *American Journal of Botany* 96, no. 10 (2009): 1767–1778. <https://doi.org/10.3732/ajb.0900041>; and Bucchi, Massimiano, and Brian Trench, eds. *Routledge Handbook of Public Communication of Science and Technology*. 3rd ed. London: Routledge, 2021.

⁹⁴ Nisbet, Matthew C., “Framing Science: A New Paradigm in Public Engagement,” in *Communicating Science*, 1st ed. (Routledge, 2009), 54–81, <https://doi.org/10.4324/9780203867631-10>.

⁹⁵ McBeth, Jones and Shanahan, “The narrative policy framework,” *supra* note 91.

⁹⁶ Cadwalladr, Carole and Emma Graham-Harrison, “Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data”. *The Guardian*, March 17, 2018. <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>

⁹⁷ Birkland, Thomas A. “Focusing Events, Mobilization, and Agenda Setting.” *Journal of Public Policy* 18, no. 1 (1998): 53–74. <http://www.jstor.org/stable/4007601>

efforts.⁹⁸ This case demonstrates that good data governance is not an abstract regulatory achievement but a life-saving one. Making these stories visible and widely understood is a political act as much as a communicative one.

5.1.5 Conclusion

Data governance will not achieve the political priority it deserves through technical excellence alone. The frameworks, norms, and institutions being developed in forums like the UNCTAD CSTD Working Group are necessary, but they are not sufficient. Without a shared public language, without narrative infrastructure, and without deliberate investment in communication strategy, data governance risks remaining what it has too often been: a conversation among specialists, conducted in a register that excludes the publics most affected by its outcomes. The lesson of climate communication is not that the problem was solved when the language improved, but that without better language, the problem could not begin to be addressed at all.

⁹⁸ Bengtsson, Linus, Xin Lu, Anna Thorson, Richard Garfield, and Johan Von Schreeb. "Improved Response to Disasters and Outbreaks by Tracking Population Movements With Mobile Phone Network Data: A Post-Earthquake Geospatial Study in Haiti." *PLoS Medicine* 8, no. 8 (August 30, 2011): e1001083. <https://doi.org/10.1371/journal.pmed.1001083>.

5.2 Whose Cloud, Whose Coffee? Designing Data Governance towards a

'Right to Knowledge' in Agrifood Systems

5.2.1 Introduction

In the mountainous coffee landscapes of Quindío, Risaralda, and Caldas in Colombia, the traditional *cultura cafetera* is meeting the invisible architecture of the digital age. Who controls the digital infrastructure behind agriculture is becoming just as important as who controls land, seed, or water. On smallholder coffee farms, farmers now generate data through certification apps, traceability platforms, and carbon tools. At the same time, coffee farming is being reshaped by digital transformation: sensors, satellite imagery, farm-management software, and AI-enabled tools are changing how production decisions are made, how traceability is verified, and how climate resilience is measured. Yet, the promise of this digital transformation is increasingly stifled by a fundamental power asymmetry: while farmers are the primary creators of value, the resulting data typically resides in proprietary, non-interoperable clouds controlled by external corporate actors.⁹⁹ This matters because a real right to knowledge is not only about access to information; it is about the ability of communities to shape how their knowledge is collected, exchanged, and used. By framing this imbalance through the lens of epistemic justice, we can better understand that a meaningful “right to knowledge” in agrifood systems requires moving beyond abstract legal ambitions toward a concrete design problem—one that embeds data interoperability, server neutrality, and community sovereignty into lived agricultural practices.

5.2.2 Context: Datafication and Power Asymmetry in Colombia

Colombia's longstanding coffee production culture draws its foundations from “principles of democratic participation, solidarity, commitment, pursuit of the common good and sustainable development.”¹⁰⁰ In recent years, however, the industry has steadily moved away from local expertise and hands-on participation toward a data-driven model known as the “digital coffee farmer.”¹⁰¹ In the coffee farms of Quindío, comprised of 5,662 farms covering over 18,000 hectares of land, we are seeing the deployment of digital technology that has turned daily, on-the-ground field observations into automated information streams.¹⁰² On farms like Las Acacias and La Morelia, digital sensors monitor critical variables such as soil moisture and air temperature to drive “smarter coffee decisions” regarding fertilization and harvest timing.¹⁰³ However, this transition is not solely driven by a desire for efficiency; it is a response to an evolving international regulatory landscape.

The European Union Deforestation Regulation (EUDR), for example, has transformed digital traceability from a voluntary sustainability effort into a mandatory condition for market access. To prove that coffee was not produced on land deforested after December 31, 2020, operators must

⁹⁹ Dalberg. Study on Data Sovereignty: Understanding the Landscape, Challenges, and Opportunities. November 2022. https://dalberg.com/wp-content/uploads/2022/11/Study_Data_Sovereignty.pdf.

¹⁰⁰ Wageningen University and Research, Coffee Sector in Colombia: Statistics and Overview (November 2024), 6, https://resiliencebv.com/wp-content/uploads/2025/03/coffee_sector_in_colombia_statistics_and_overview-wageningen_university_and_research_686996.pdf.

¹⁰¹ “Digital Coffee Farmer: IoT Sensors and AI for Smarter Coffee Decisions.” Colombia One: News from Colombia and the World. December 19, 2025. <https://colombiaone.com/2025/12/19/digital-coffee-farmer-iot-sensors-ai-coffee-farming/>.

¹⁰² *Ibid.*

¹⁰³ *Ibid.*

now provide precise geolocation data.¹⁰⁴ While the legal responsibility for this due diligence lies with EU-based buyers, the actual burden of data collection, cleaning, and verification is shifted "upstream" to producers and cooperatives who often lack the technical resources to comply independently. The EU's emerging Digital Product Passport (DPP) agenda suggests that this shift towards digitised compliance is not limited to forest-risk commodities.¹⁰⁵ As product-level digital records become central to sustainability claims, traceability, and market access, they also raise a fundamental governance question: who controls the underlying data, who can update it, and who benefits from its use?

Herein lies a profound power asymmetry. These regulations are undeniably important for addressing deforestation and ensuring sustainable supply chains, but the burden of compliance should not fall disproportionately on smallholder farmers—it should be borne by the powerful corporations who design the standards, control the platforms, and benefit from the market premiums. Under the existing model, smallholders find themselves locked into corporations' proprietary clouds and non-interoperable platforms, compelled to feed data upward while gaining little reciprocal access to aggregated insights or decision-making authority. This creates an environment where smallholders are treated as mere data sources for downstream actors rather than active participants in a knowledge commons. Ultimately, this structural imbalance represents a clear case of epistemic injustice. As defined by the Intergovernmental Science-Policy Platform on Biodiversity and Ecosystem Services (IPBES), this involves "distributive unfairness" in the management of knowledge goods and disputes over what information counts as valid in decision-making.¹⁰⁶ Without intervention, the datafication of coffee risks turning local territories into sites of wealth and information extraction, all while limiting the smallholder's right to derive knowledge from the very land they sustain.

5.2.3 Proposal 1: Data Interoperability as a Knowledge Commons

The technical foundation of any meaningful "right to knowledge" in the agrifood sector must be data interoperability. One layer of interoperability, in its simplest form, is the ability to exchange and make use of data between different devices and systems. In practice, this means moving beyond isolated digital tools toward shared standards, open formats, and common protocols that allow information to travel securely across platforms without being repeatedly re-entered, re-verified, or trapped in proprietary systems.¹⁰⁷ The transition to a knowledge commons can draw inspiration from Digital Public Infrastructure (DPI) models like the India Stack or Ethiopia's FarmStack.¹⁰⁸ These systems are designed to be "secure and interoperable, built on open technologies" to provide equitable access to services at a societal scale.¹⁰⁹ In Ethiopia, the FarmStack protocol facilitates trusted data transfers, allowing farmers to give consent for their data to be shared across a range of partners rather than

¹⁰⁴ Viladrich Beiroa, Oscar. 2025. "Digital Solutions for Smallholder Cooperatives under the European Union Deforestation Regulation: A Case Study in Ivory Coast." https://essay.utwente.nl/fileshare/file/109147/Oscar_Viladrich%20-%20Digital%20solutions%20for%20smallholder%20Cooperatives%20under%20the%20EUDR.pdf.

¹⁰⁵ GS1 Switzerland, "Digital Product Passport," <https://www.gs1.ch/en/products-services/digital-product-passport>.

¹⁰⁶ "Epistemic Justice | IPBES Secretariat." 2024. IPBES Secretariat. <https://www.ipbes.net/glossary-tag/epistemic-justice>.

¹⁰⁷ "Building Data Interoperability in Agriculture - Farm Foundation." Farm Foundation. October 16, 2023. <https://www.farmfoundation.org/projects/building-data-interoperability-in-agriculture/>.

¹⁰⁸ See Hansberry, Cate. "Global DPI Models: Lessons from India, Brazil, and Beyond." Atlantic Council. October 25, 2024. <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/global-dpi-models-lessons-from-india-brazil-and-beyond/> (for India Stack); see also Dalberg, Study on Data Sovereignty, *supra* note 99 (for Ethiopia's FarmStack).

¹⁰⁹ Cate Hansberry, "Global DPI Models," *supra* note 108.

being locked into a single relationship.¹¹⁰ These frameworks allow local cooperatives to connect their internal management systems directly to international markets without losing ownership of the underlying information. Ultimately, interoperability is not just a technical fix; it is an empowerment tool.¹¹¹ In Colombia and other coffee-producing regions, it is the precondition that ensures the "digital coffee farmer" is not just a source of information for an AI model in the Global North, but a primary participant in a global, equitable knowledge commons.

5.2.4 Proposal 2: Data Server Neutrality and Stewardship

The second data governance design proposal expands upon interoperability to ensure that the companies hosting agrifood data act as neutral caretakers of information rather than gatekeepers. This principle, which we will call "data server neutrality," argues that the entities storing and routing agricultural information should not use their powerful position to lock in users or extract unfair value from the data they simply steward.

A major concern arises when a single corporation plays too many roles at once. For example, in some Colombian projects, a single tech giant might act as the cloud provider, the buyer of carbon credits, and the primary technology partner.¹¹² This vertical integration creates, once again, a power imbalance, making it difficult for farmers to move their business elsewhere and leaving them dependent on a platform they do not control.¹¹³

To achieve epistemic justice, we must move toward a stewardship model. Traceability platforms such as Beyco illustrate this shift by utilizing technology to grant farming cooperatives "full ownership of their data."¹¹⁴ This allows local groups to create offers with greater negotiation power and connect with international buyers independently rather than being stuck in one company's system.

Neutrality rules, modeled on the EU's Data Governance Act,¹¹⁵ would mandate:

- No exclusive lock-ins: farmers can switch platforms without data loss;
- Separation of roles: hosts cannot also act as buyers or analytics providers;
- Transparent access: equal terms for all users, regardless of size or buyer relationship.

By design, server neutrality transforms data from a corporate asset into a communal one, ensuring smallholders remain primary decision-makers over their knowledge.

5.2.5 Proposal 3: Protecting Social and Community Sovereignty Interests

The final proposal for a meaningful "right to knowledge" in agrifood is social and community sovereignty: the principle that local communities and their regional institutions must have the power

¹¹⁰ Dalberg. Study on Data Sovereignty, *supra* note 99.

¹¹¹ "Building Data Interoperability in Agriculture - Farm Foundation," *supra* note 107.

¹¹² See FIAN, "Coffee and Carbon in Colombia: Human Rights Concerns at the Intersection of Food Systems, Climate Change and Data-Based Technologies." 2024. FIAN International. [https://www.fian.org/files/is/htdocs/wp11102127_GNIAANVR7U/www/files/Coffee_Carbon_Markets_20240624_abfin\(2\).pdf](https://www.fian.org/files/is/htdocs/wp11102127_GNIAANVR7U/www/files/Coffee_Carbon_Markets_20240624_abfin(2).pdf). for more info on the Asómbate project in Colombia and its connection to Microsoft.

¹¹³ "Empowering Coffee Cooperatives with Digital Data Management: A Case Study on Carbon Insetting and Traceability Using the Beyco Platform in Colombia." n.d. Solidaridad Network. Accessed April 12, 2026. https://www.solidaridadnetwork.org/wp-content/uploads/2025/12/Empowering-Coffee-Cooperatives-with-Digital-Data-Management_Solidaridad.pdf.

¹¹⁴ "Beyco." Beyco.nl. 2026. <https://beyco.nl/>.

¹¹⁵ European Commission. "Data Governance Act | Shaping Europe's Digital Future." Digital-Strategy.ec.europa.eu. 2023. <https://digital-strategy.ec.europa.eu/en/policies/data-governance-act>.

to set the rules for their own information.¹¹⁶ Any real right to knowledge must recognize that the digital representation of a farm is inseparable from the territory and the people who sustain it.¹¹⁷ In Colombia, groups like the National Federation of Coffee Growers (FNC) are already updating georeferencing data to help farmers meet new regulations, showing how local institutions can act as guardians of producer interests.¹¹⁸ True sovereignty is built on more than just a “consent” button; it requires a foundation of awareness, access, and literacy so that farmers can truly understand the value of the data they are sharing.¹¹⁹

As Michael Fakhri, former United Nations Special Rapporteur on the Right to Food, notes in his report *“Corporate power and human rights in food systems,”* it is not always more data that is needed to strengthen digitalization efforts, “but better governance systems that ensure the power of data generation and dissemination is in the hands of the people generating those data, which in turn is used to realize the human rights of communities and Indigenous Peoples.”¹²⁰

This framing positions sovereignty as a collective right grounded in self-determination, where authority over data is linked to the preservation of cultural identity, knowledge systems, and community governance structures. In this sense, social and community sovereignty also conceptualizes data as an extension of individual and collective ethical agency, enabling communities to exercise authority over how their information is collected, used, and commercialized with consideration for the broader social and political implications of agribusiness. By centering community agency, we ensure that the digital transformation of coffee does not become a new form of “data colonialism,” but instead respects the right of rural people to determine their own digital futures.

5.2.6 Conclusion

International policymakers would be wise to advocate for data interoperability, server neutrality, and social and community sovereignty as baseline principles for agrifood digital infrastructures. These design requirements work to promote and realize a tangible right to knowledge.

The three proposals laid out in this article converge in a modern knowledge ecosystem rooted at the heart of agricultural production: interoperability repatriates local knowledge, neutrality ensures equitable access, and sovereignty grounds information sharing in accountability and informed consent.

The digitized future of coffee production at once highlights a unique challenge and illuminates a scalable solution. The Colombian coffee industry is used here as a case study; the three proposals set forth in this article can be adapted and implemented across commodities and regions. By designing international data governance frameworks that prioritize interoperability, neutrality, and sovereignty, smallholder agrifood systems worldwide can begin to reclaim their epistemic agency.

¹¹⁶ For more in-depth framing of Social and Community Sovereignty, see *supra* Section 3 of this report: Analytical Brief: Reconciling Sovereignty and Interoperability in Data Governance

¹¹⁷ FIAN, “Coffee and Carbon in Colombia,” *supra* note 112.

¹¹⁸ “Colombia Launches Traceability Platform in September.” Tridge. September 4, 2024. <https://www.tridge.com/news/colombia-launches-traceability-platform-in-s-hfdoar>.

¹¹⁹ Dalberg. Study on Data Sovereignty, *supra* note 99.

¹²⁰ Fakhri, Michael. “Report of the Special Rapporteur on the Right to Food, Michael Fakhri: Corporate Power and Human Rights in Food Systems.” UN.org, United Nations General Assembly, 21 July 2025, docs.un.org/en/A/80/213, page 11.

5.3 Strengthening Indigenous Data Sovereignty and Knowledge Co-Production: Addressing Inequalities in Global Data Governance

5.3.1 Introduction

During the 5th meeting of the UN CSTD Working Group on data governance in February 2026, several speakers highlighted significant gaps in current approaches to global data governance frameworks.¹²¹ More specifically, the insufficient consideration of data colonization, misuse and misappropriation, as well as the structural inequalities shaping global data ecosystems. These asymmetries of capacities, especially between countries of the Global North and the Global South, contribute to increase digital divides and limitate the ability of certain communities to control, access and benefit from their own data.

These challenges are especially faced by Indigenous communities, whose knowledge systems are increasingly digitized, shared and integrated into global data infrastructures without adequate protections or recognition of their rights. While new technologies offer opportunities for preserving and disseminating Indigenous knowledge, it also exposes communities to risks of exploitation and cultural dislocation. Therefore, there is a need to develop new principles to strengthen the ownership of Indigenous communities on their own data, by establishing protective standards within international law and global governance frameworks. In this context, this article questions how can a global data governance framework better integrate Indigenous data sovereignty and knowledge co-production to ensure equitable and rights-based management of Indigenous knowledge?

The article will first examine the structural inequalities and risks associated with the current data ecosystem, before exploring the nature of Indigenous knowledge and the existing legal and ethical frameworks that seek to protect it. Then, the article will present knowledge co-production as a transformative approach to research and governance of Indigenous data. Finally, it proposes a pathway toward more inclusive and equitable data governance frameworks relevant for the UN CSTD Working Group discussion.

5.3.2 An Unequal Data Landscapes: Structural Inequalities and Risks of Misappropriation of Indigenous Data

Insights from the UN Data Working Group:

As previously mentioned, this article builds upon the discussions held within the UN Data Working Group on the need to better address global inequalities in data governance frameworks. Several delegations highlighted several persistent challenges such as The Gambia, who mentioned unresolved issues regarding the digital divide, resource constraints, the risks of data colonisation and the insufficient recognition of Indigenous data rights. On a same note, Cuba stressed the importance of recognizing structural inequalities and the need to end technological dependency through capacity-building, while condemning data colonization and the coercive uses of data.

¹²¹ United Nations Conference on Trade and Development (UNCTAD). "5th Meeting of the UN CSTD Multi-stakeholder Working Group on Data Governance at All Levels." Accessed April 11, 2026.

Several delegations also underscored the importance of cultural and linguistic diversity and the implementation of safeguards in data use. The Organisation Internationale de la Francophonie (OIF) especially pointed out the lack of attention given to the digital divide and the absence of key concepts such as cultural and linguistic diversity in current frameworks.

Recommendations from these delegations included integrated equity principles, strengthening Global South perspective and developing hybrid governance frameworks adaptable to diverse cultural contexts. These contributions highlight the need for a more inclusive and representative approach to global data governance that reflects the realities and priorities of underrepresented regions and communities.

Data Colonization and Extractivism:

The risks identified by the Working Group can be understood through the concept of data colonization and data extractivism. Data colonization refers to situations in which powerful actors, often private technology companies, appropriate data generated by others, particularly in low and middle income countries and capture most of its value. Similarly, data extractivism reflects a continuation of colonial patterns of resource extraction, where communities have little control on how their data are collected, used or monetized.¹²²

These dynamics manifest across a variety of sectors and dimensions of inequality including access to data and technologies, asymmetries of information, ownership over data, value distribution, accountability mechanisms and the adequate representation of knowledge. Without adequate governance safeguards, these practices reinforce existing power imbalances and marginalize Indigenous knowledge.

The Need for Data Equity Across the Data Lifecycle:

Addressing these challenges requires embedding equity throughout the entire data lifecycle, from collection to storage, analysis and dissemination. It includes ensuring that Indigenous communities retain control over how their knowledge is interpreted and shared. Safeguarding Indigenous knowledge requires protection against illicit access and misuse while enabling communities to define access conditions, annotation of data in their own languages and maintaining the cultural context of their knowledge.¹²³

5.3.3 Strengthening Indigenous Knowledge and Rights: The Foundations for an Equitable Governance of Data

Understanding Indigenous Knowledge Systems:

¹²² Sabrina McCutchan, *Research Data Governance for Global Health: A Landscape Analysis*, Version 1.1 (Durham, NC: Duke Global Health Institute, September 26, 2022).

¹²³ Amy Hawn Nelson, "Centering Community Involvement and Equity Across the Data Life Cycle," *Harvard Data Science Review*, no. Special Issue 2 (2021).

Indigenous knowledge can be defined as deeply embedded in community practices, cultural traditions and relationships within specific territories. It is rooted in particular environments and is often difficult to codify as it is mainly transmitted orally through storytelling, observation and practice. Indigenous knowledge is dynamic and constantly evolving, and encompasses diverse forms of expression including folklore, rituals, craftsmanship and interactions with the natural world. These various features and languages are often overlooked in conventional data governance systems.¹²⁴

Legal and Ethical Frameworks for Indigenous Data Protection:

Existing frameworks provide foundations for protecting Indigenous knowledge and data. The indigenization of research especially emphasizes the recognition of self-determination rights of Indigenous communities and their rights to direct participation in research processes.¹²⁵ Strengthening Indigenous Data Sovereignty refers to asserting the rights of Indigenous peoples to own, control, access and manage their data related to their territories and knowledge systems.¹²⁶

Legal and ethical instruments are emerging to protect Indigenous knowledge and data, such as new privacy laws to protect the individual right to privacy. For instance, the European Union's General Data Protection Regulation (GDPR)¹²⁷ outlines individual privacy rights, consent processes, data protection principles, accountability frameworks as well as the "right to be forgotten". Similarly, Canada established the OCAP principles (Ownership, Control, Access, Protection)¹²⁸ to protect Indigenous intellectual property by strengthening Indigenous control over data collection. While the CARE principles for Indigenous Data Governance¹²⁹ were created in 2019 by the International Indigenous Data Sovereignty Interest Group,¹³⁰ to outline collective rights related to open data. The acronym refers to the share of collective benefits, the authority and responsibility to control data.

However, even though broader legal instruments such as privacy laws and right to informed consent mechanisms offer some protections, it remains insufficient as they tend to prioritize individual rather than collective rights.¹³¹ This highlights a key tension: while existing frameworks provide partial protection, they must be expanded to fully recognize collective ownership and cultural specific governance mechanisms.

5.3.4 Knowledge Co-Production: A Collaborative and Transformative Approach to Strengthen Indigenous Data Sovereignty

¹²⁴ Sen, Bharati. "Indigenous Knowledge for Development: Bringing Research and Practice Together." *International Information & Library Review* 37, no. 4 (2005): 375–382.

¹²⁵ Victoria N. Sharakhmatova, "Indigenous Knowledge Data Management Issues and Co-Production of Knowledge in Kamchatka," *Data Science Journal* 20, no. 1 (2021): 1–10.

¹²⁶ Sabrina McCutchan, *supra* note 122.

¹²⁷ European Union, *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, Official Journal of the European Union L119 (2016): 1–88.

¹²⁸ First Nations Information Governance Centre, *The First Nations Principles of OCAP®: Ownership, Control, Access and Possession* (Ottawa: FNIGC, 2014).

¹²⁹ Research Data Alliance International Indigenous Data Sovereignty Interest Group, CARE Principles for Indigenous Data Governance (Global Indigenous Data Alliance, 2019).<https://www.gida-global.org/care>

¹³⁰ Research Data Alliance International Indigenous Data Sovereignty Interest Group, *International Indigenous Data Sovereignty Interest Group*, accessed April 11, 2026.<https://www.rd-alliance.org/groups/indigenous-data-sovereignty-ig>

¹³¹ Sabrina McCutchan, *supra* note 122.

Rethinking Knowledge Production:

Knowledge co-production can be defined as a collaborative research practice that seeks to co-produce actionable knowledge with Indigenous communities. It combines traditional knowledge with scientific research methods to develop solutions that are both scientifically robust and culturally relevant. This approach challenges the dominant western epistemology by removing barriers to Indigenous self-determination and decentering traditional academic institutions as the only producers of knowledge. Indigenous epistemologies and practices are valued, enabling traditional owners to define and control their rights, by contextualizing and annotating resources in their own language.¹³²

However, barriers to co-produce remain both material and discursive as the lack of recognition, funding and infrastructures remain persistent challenges.

Case Studies and Innovations: The Contribution of Ethnographic Research in Identifying Good Practices

Innovations in Indigenous Knowledge and knowledge co-production are not restricted to academic literature but actually take place in the field.¹³³ Several empirical examples demonstrate the potential of knowledge co-production to enhance community empowerment.

In India, initiatives such as the Traditional Knowledge Digital Library (TKDL)¹³⁴ and the Community Biodiversity Registers¹³⁵ document and protect Indigenous knowledge while ensuring their participation. Indian NGOs are actively building upon traditional ecological knowledge to decentralize governance through the People's Ecological Planning (PEP).¹³⁶ The Honey Bee Network¹³⁷ also represents a grassroots initiative gathering practices learnt from the people, identifiable and shared in their own languages.

In Kamchatkan, the UN conservation projects integrated Indigenous Knowledge into environmental governance through several educational programs and cultural initiatives. The project fostered dialogue between scientific knowledge and Indigenous practices through ethno-ecological camps, festivals, creative competitions and manuals on Indigenous language and culture. Cartographical and GIS technologies such as community-based mapping, have enabled communities to document their knowledge and assert territorial rights.¹³⁸ The Federal Register of Intangible Cultural Heritage Objects was created in 2010 in Russia to preserve cultural heritage including oral creativity, traditions, forms

¹³² Victoria N. Sharakhmatova, *supra* note 125.

¹³³ Estabrooks, Carole A. "Reflections on Co-production as a Mode of Knowledge Production: Comment on 'Research Coproduction: An Underused Pathway to Impact.'"

¹³⁴ Council of Scientific and Industrial Research (CSIR), Government of India, *Traditional Knowledge Digital Library (TKDL)*, accessed April 11, 2026. <https://culture.gov.ru/>

¹³⁵ Government of India, Ministry of Environment and Forests, *Community Biodiversity Registers: Guidelines for Documentation of Biodiversity at Local Level* (New Delhi: Government of India, 2009).

¹³⁶ Sen, Bharati. "Indigenous Knowledge for Development: Bringing Research and Practice Together." *International Information & Library Review* 37, no. 4 (2005): 375–382.

¹³⁷ Society for Research and Initiatives for Sustainable Technologies and Institutions (SRISTI), *The Honey Bee Network*, accessed April 11, 2026, honeybee.org.

¹³⁸ Victoria N. Sharakhmatova, *supra* note 125.

of expressions and dialects, while defining the rights of bearers, guardians, individuals and legal entities.¹³⁹

Methods for the Digitization of Indigenous Data:

The digitization of Indigenous Knowledge presents both opportunities and risks. Ethnographic research and recent knowledge co-production processes aim to use digital tools such as databases, GIS systems and multimedia platforms to enhance accessibility and preservation.¹⁴⁰

Responsible Indigenous data management therefore requires a controlled and context sensitive access to data, rights-based governance protocols, secure infrastructures and flexible tools supporting oral traditions and cultural specificities. Security measures can include encryption, digital signature or flexible software tools supporting oral traditions.

Firstly, the treatment of traditional knowledge must be identified through the technical and social analysis of communities' practices. Indigenous knowledge then needs to be validated and documented in terms of relevance and functionality. Knowledge must be secured through electronic storage and applications to guarantee access. Finally, the dissemination of Indigenous Knowledge through publications and awareness campaigns is crucial to ensure the exchange of knowledge between communities.

Adequate digital tools must also be used for the relevant data and documentation. Based upon existing ethnographic works, computer technology is often used to address natural resources and ecosystem problems. Meanwhile GIS systems, implemented by locals, are useful to consolidate, store and analyze their data. As shown previously, mapping and ethnographic cartographies are tools asserting greater political autonomy and preserving Indigenous cultural heritage. Another relevant technique is counter-mapping, which refers to maps challenging dominant power structures by including communities that are usually excluded from exercising control over their own land or knowledge.

5.3.5 Toward an Inclusive and Equitable Data Governance Framework

Hybrid and Equity-Centered Governance Models:

Building a more inclusive data governance framework requires moving beyond a one size fits all approach. There is a need for hybrid models that combine international standards with locally grounded governance practices, offering greater flexibility and responsiveness to diverse community needs.

Therefore, it is crucial to challenge western centric approach to ownership, especially as intellectual property laws are centered on individual rights. However, strengthening the ownership of Indigenous Knowledge requires a system based on collective rights, emphasizing the importance of collective

¹³⁹ Ministry of Culture of the Russian Federation, *Federal Register of Intangible Cultural Heritage Objects* (Moscow: Government of the Russian Federation, 2010), accessed April 11, 2026. <https://culture.gov.ru/>

¹⁴⁰ Victoria N. Sharakhmatova, *supra* note 125.

identities, cultures. Intellectual property rights need to vary among diverse communities as well as data sizes. An inherent flexible and scalable data governance framework can include new systems for distributing data rights to community stakeholders by establishing local cooperatives or licensing exclusive rights to local communities.¹⁴¹

Capacity-Building and Technological Empowerment:

In order to address structural inequalities, sustained investments are required in building local data infrastructures, technical and institutional capacity as well as Indigenous-led research initiatives. Empowering communities to manage their own data systems is essential to reduce dependency and ensure the preservation of cultural heritage.

Safeguards, Protocols and System Design:

A robust governance framework must also include safeguards and technical mechanisms. The architecture of a protective framework should include a metadata system, where traditional owners provide access and usage conditions. Appropriate protection measures should secure databases, including non-patent databases. Interfaces must support diverse data formats (audio, visual, textual) and management protocols must ensure accountability and traceability.¹⁴² Such systems must be designed with flexibility and scalability in mind, to reflect the diversity of Indigenous knowledge systems.

5.3.6 Conclusion

In conclusion, this article argued that strengthening Indigenous data sovereignty and promoting knowledge co-production, are essential components of equitable data governance frameworks. Current systems are shaped by structural inequalities, asymmetric power relations and often fail to protect Indigenous data or ensure fair distribution of benefits. Addressing these challenges requires a shift toward governance models centering Indigenous rights, recognizing collective ownership and fostering collaboration between scientific research and local communities. Integrating equity, flexibility and participation into data governance frameworks enable to better support the preservation, protection and sustainable use of Indigenous knowledge. Ultimately, advancing Indigenous data sovereignty constitutes a critical step toward a more inclusive, pluralistic and sustainable global data ecosystems.

¹⁴¹ Latulippe, Nicole, and Nicole Klenk. "Making Room and Moving Over: Knowledge Co-production, Indigenous Knowledge Sovereignty and the Politics of Global Environmental Change Decision-Making." *Current Opinion in Environmental Sustainability* 42 (2020): 7–14.

¹⁴² Sen, Bharati. "Indigenous Knowledge for Development: Bringing Research and Practice Together." *International Information & Library Review* 37, no. 4 (2005): 375–382.

5.4 Embedding Human Rights and Data Justice in Health Data Governance

5.4.1 Introduction

The growing availability of real-time data, advanced analytical tools and large-scale datasets has transformed the health sector in recent years. These developments have helped improve disease prevention, diagnosis, treatment and care delivery while enabling policy makers to better understand the social determinants of health. At the same time, the rapid expansion of technologies in the health sector has increased the risks of data breaches, inappropriate data-sharing and misuse of sensitive information.

Health data can be defined as data related to the physical or mental health of individuals used to support health decisions. Health data has become a highly sensitive information, raising concerns about its exploitation for political, economic or discriminatory purposes. Health Data Governance (HDG) refers to the set of processes and frameworks regulating the management and the use of health data. The COVID19 pandemic exposed existing fragilities of the Health Data Governance system, revealing structural inequalities and human rights challenges. The establishment of new safeguards lies at the center of contemporary debates around Health Data Governance.

Therefore, this article questions how Health Data Governance frameworks can better integrate human rights and data justice principles to ensure equitable, secure and accountable use of health data?

Firstly, the article will examine how Health Data Governance frameworks were put under pressure during the COVID19 pandemic, exposing the ineffective cooperation between states, the erosion of civil liberties and structural inequalities in accessing health data and technologies. Secondly, the article will discuss the foundations of a global health data governance framework grounded in human rights, as well as policy recommendations and operational pillars that need to be implemented. Finally, the article will stress the importance of adopting a dual lens approach, using both human rights and data justice concepts to build an equitable and sustainable health data governance framework.

5.4.2 Health Data Governance Under Pressure: Lessons from the COVID-19 Pandemic

Expansion of Surveillance and Erosion of Civil Liberties:

The COVID-19 pandemic has raised unprecedented concerns in the collection and use of health-related data, especially regarding data privacy, access and risks of data breaches. Based on the Siracusa Principles¹⁴³ established in 1984, states are entitled to base their health decisions on scientific standards and to choose the least restrictive alternatives. Yet, during the pandemic, many states used vast emergency powers, undermining fundamental rights. Digital surveillance tools, such as contact tracing, geolocation tracking and biometric monitoring were deployed at scale and

¹⁴³ United Nations Economic and Social Council. *The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights*. UN Doc. E/CN.4/1985/4, 1984.

violated human rights. Governments used COVID-19 as an excuse to expand and normalize their surveillance powers, as systems relying on big data analytics enabled authorities to monitor population movements and enforce public health measures.

In some cases, governments even used the pandemic to justify broader political repression. In China, Wuhan officials concealed early data, silenced truth-tellers and conducted intrusive surveillance, violating civil and political rights. This is an illustration of how health emergencies can be instrumentalized to consolidate power.

Public health measures frequently resulted in significant restrictions of civil and political rights. Across multiple countries, journalists and healthcare workers were arrested for criticizing governmental responses, while access to accurate health information was constrained. These restrictions included disinformation, arbitrary detention, restrictive access to life-saving medical care and limitations on freedom of movement, assembly and expression. Such practices not only endanger human rights but also weaken public health outcomes by reducing transparency and trust.

Fragmented Global Cooperation and Governance Gaps:

Health data are governed by a wide range of international, regional and national legal and regulatory instruments, policies and norms. However, the pandemic highlighted major deficiencies in international cooperation on health data. Existing legal frameworks, including the International Covenant on Economic, Social and Cultural Rights (ICESCR)¹⁴⁴ lack precise obligations regarding what the “international assistance and cooperation” entails.

Geopolitical tensions further undermined collaboration due to limited transparency in data reporting, a lack of cooperation with the World Health Organization (WHO) investigations and an unequal vaccine distribution. Structural challenges included an absence of interoperable health data standards or clear protocols for data-sharing. Coordination between the national health system was weakened due to the absence of cross-departmental and cross-border data-sharing associated with clinical research, telemedicine and Artificial Intelligence (AI). These gaps significantly undermined the effectiveness of a global response to the pandemic and reduced the potential benefits of interoperable health data systems.

Inequalities in Access to Health Data and Technologies:

The COVID-19 pandemic exposed and exacerbated structural inequalities in the right to health. In accordance with article 12.1 of the Covenant¹⁴⁵, states recognize “*the right of everyone to the enjoyment of the highest attainable standard of physical and mental health*”. However, the digital divide limited access to essential information and participation in data driven health systems. Marginalized communities, particularly racial minorities, Indigenous populations and migrant workers were disproportionately affected due to unequal access to healthcare services and digital resources. In the United States, Black Americans and Latino populations died twice the rate of white

¹⁴⁴ United Nations General Assembly. *International Covenant on Economic, Social and Cultural Rights (ICESCR)*. Adopted December 16, 1966. United Nations Treaty Series 993 (1976): 3.

¹⁴⁵ *Ibid*, Article 12(1).

citizens, while migrant workers were forced to live in condensed areas, sanitary at higher risks. Globally, the rights of women and children were also burdened, especially concerning access to education, work and justice.

Meanwhile, high income countries secured preferential access to vaccines and medical technologies through purchase agreements, such as the “vaccine purchase agreements,” undermining the principle of health as a global common good. Intellectual property regimes also constituted an obstacle to the equitable distribution of life-saving resources, reinforcing global disparities.

5.4.3 Limits of Human Rights-Based Health Data Governance

Emerging International Initiatives Centering Human Rights as a Foundational Framework:

Human Rights Law provides an essential framework to safeguards against the misuse of health data and the normalization of intrusive surveillance. Principles such as necessity, proportionality and accountability must guide health data practices. The Siracusa Principles¹⁴⁶ established strict conditions under which rights may be limited, emphasizing that restrictions must be necessary, proportionate and non-discriminatory.

Several international initiatives have recognized the need for a coherent health data governance framework:

- OECD Recommendation on Health Data Governance (2017)¹⁴⁷
- Transform Health Coalition (2020)¹⁴⁸
- WHO Global Strategy on Digital Health (2020-2025)¹⁴⁹
- WHO Health Data Governance Summit (2021)¹⁵⁰

These initiatives highlight the importance of shared standards, international cooperation and the ethical use of health data. As an example, The Health Data Governance Principles¹⁵¹ established by the Transform Health Coalition in 2020, were endorsed by 130 national, regional and international organizations and aim to bring a human rights lens to the governance of health data around three pillars. Firstly, the protection of individual rights, by establishing safeguards against data exploitation, discrimination, surveillance and neocolonialism. Secondly, the promotion of health value through responsible data-sharing supporting innovation and public health. Finally, advancing equity, by enabling public engagement, education and the meaningful participation of all groups. It includes mitigating data bias and the prioritization of marginalized groups. However, although widely endorsed, these principles require stronger mechanisms for implementation and accountability, as

¹⁴⁶ United Nations Economic and Social Council. *The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights*. UN Doc. E/CN.4/1985/4, 1984.

¹⁴⁷ Organisation for Economic Co-operation and Development (OECD). *Recommendation of the Council on Health Data Governance*. Paris: OECD, 2017.

¹⁴⁸ Transform Health Coalition. *Transform Health Coalition Principles for Health Data Governance*. 2020.

¹⁴⁹ World Health Organization, *WHO Guidance on Ethics and Governance of Artificial Intelligence for Health* (2021).

¹⁵⁰ World Health Organization. *Health Data Governance Summit: Summary Report*. Geneva: World Health Organization, 2021.

¹⁵¹ Transform Health Coalition. *Health Data Governance Principles*. 2020. <https://transformhealthcoalition.org/areas-of-focus/health-data-governance/>

human rights law still appears as a field of contestation. It can be used both as a language of hegemony or counter-hegemony, meaning it can be used as a legitimization tool for state power.

Remaining Gaps in the Implementation of Human Rights in Health Data Governance Frameworks:

Effective governance now must translate existing principles into concrete mechanisms. Concrete mechanisms should include informed consent, which describes a revocable consent process with special protections for vulnerable populations.¹⁵² Data access must include transparent procedures and safeguards against data commodification. The use of appropriate metrics would also ensure a fair representation of datasets through the geographic locations of data. The securitization of controls involve secure data storage, remorse-delete software and the identification of sensitive data. Finally, a clear identification of responsibility and accountability mechanisms are necessary to ensure compliance with regulations.¹⁵³

Additionally, to strengthen the integration of human rights into health data governance, several actions are necessary to ensure the equitable distribution of medical technologies. To do so, the World Trade Organizations should waive intellectual property protection and equitable distribution facilities¹⁵⁴. The International Health Regulations¹⁵⁵ needs to be revised to develop specific standards for confidentiality, privacy and the protection of whistleblowers. A “right to health information” appears to be necessary to combat misinformation, especially during pandemics and it could be supported by the adoption of a World Health Assembly (WHA) resolution and health literacy campaigns from civil society.¹⁵⁶ A global funding mechanism, such as for instance an International Financing Facility, is also necessary to strengthen the global health system responses to emergencies. Similarly, a “right to health capacity fund” could support civil society to advance the right to health advocacy.¹⁵⁷

To improve national and global health and rights architecture, the adoption of a Framework Convention on Global Health¹⁵⁸ would establish mechanisms and a regime of accountability. The establishment of health equity programmes of action would set actions across the various determinants of health. Finally, the adoption of a pandemic treaty integrating human rights has been heavily discussed following the COVID-19 and aims to protect individuals and marginalized groups’ rights from state over-reach, global stockpile and data openness.¹⁵⁹

5.4.4 Toward a Data Justice Approach to Health Data Governance

¹⁵² World Health Organization, *Ethics and Governance of Artificial Intelligence for Health: WHO Guidance (PDF)*.

¹⁵³ Tiffin, Nick, and George LeFevre. *How to Use Relevant Data for Maximal Benefit with Minimal Risk: Digital Health Data Governance to Protect Vulnerable Populations in Low-Income and Middle-Income Countries*.

¹⁵⁴ Katrina Perehudoff et al., “Improving Access to COVID-19 Vaccines,” *Health and Human Rights Journal*, December 6, 2022.

¹⁵⁵ World Health Organization, “International Health Regulations (IHR),” accessed April 11, 2026. <https://www.who.int/health-topics/international-health-regulations/>

¹⁵⁶ Danielle Muscat et al., “Universal Health Information Is Essential for Universal Health Coverage,” *Family Medicine and Community Health* 11, no. 2 (2023).

¹⁵⁷ Lawrence O. Gostin, “Human Rights and the COVID-19 Pandemic,” *Journal of the American Medical Association* 323, no. 24 (2020): 2470–2471. <https://doi.org/10.1001/jama.2020.6647>.

¹⁵⁸ Framework Convention on Global Health (FCGH) Alliance, “Framework Convention on Global Health,” accessed April 11, 2026. <https://fcghalliance.org/>.

¹⁵⁹ Lawrence O. Gostin, *supra* note 157.

From Data Governance to Data Justice:

This article argues that the protection of the right to health extends beyond the mere technical governance of health data. It is necessary to address structural inequalities embedded in the current data systems and adopt a dual lens with human rights and Data Justice. The concept of Data Justice refers to frameworks which contribute to redress structural inequalities by promoting fairness, inclusion and the equitable participation in health systems. It is a solidarity-based approach to data for health, emphasizing on the collective benefits while giving people greater control over their own data. Several urgent issues must be addressed through the lens of Data Justice such as health data colonialism and the exploitation of data in low income countries, as well as the commercialization of health data and the biases of representation in datasets.

Expanding the Definition of Health Data:

To address these challenges, there is a growing recognition that health data should be defined more broadly. Health Data Governance frameworks are increasingly establishing a distinction between “health-related data” and “health-related uses of data” to address larger issues such as the commercialization of health data. As an example the EU General Data Protection Regulation (GDPR) defined in 2016, health-related data as any “data concerning health,” therefore including data from any sources. Health-related data refer to the data collected in the contexts of public health and healthcare, while health related uses of data include data collected in other contexts such as digital commerce or social media.

Data Justice approach thus requires a multi-layers governance of health data which include the protection of individual ownership but also collective ownership. Both personal control and group rights need to be respected and protected. Protections must be granted by norms of institutional control, for health organizations in possession and control of health data. Finally, international cooperation on the harmonization and adoption of global standards, as well as the establishment of clear obligations for the private sector through norms of public-private partnerships are necessary to ensure an equitable, sustainable and accountable health governance system.

5.4.5 Conclusion

In conclusion, the COVID-19 pandemic has demonstrated both the transformative potential of health data and the profound risks associated with its misuse. Weak governance frameworks, fragmented international cooperation and structural inequalities undermine the ability of health data systems to deliver equitable and rights-based outcomes.

Embedding human rights and data justice into health data governance is therefore not merely a normative aspiration but an urgent necessity. A global framework grounded in principles such as equity, accountability and solidarity can ensure that health data serves the public good, while protecting individual and collective rights.

Addressing these challenges requires greater coordination between health actors, at the international, regional and local levels, through the establishment of legal protections and inclusive governance mechanisms centering the voices of marginalized communities. Only such an approach can make health data governance models contribute to more equitable, resilient and effective global health systems to guarantee the right to health.

6.1 Analysis of Key Terms Across Working Group Submissions

The word cloud features the following terms:

- governance**
- data**
- principles**
- development**
- response**
- united**
- tensions**
- context**
- international**
- technical**
- framework**
- different**
- promote**
- balancing**
- society**
- effective**
- standards**
- individuals**
- diversity**
- member**
- environmental**
- safeguards**
- principle**
- value**
- republic**
- ensuring**
- harm**
- private**
- stakeholders**
- infrastructure**
- sustainable**
- power**
- ethical**
- national**
- right**
- including**
- cross-border**
- tension**
- core**
- general**
- sector-specific**
- control**
- countries**
- open**
- particularly**
- legal**
- ensure**
- relevant**
- strong**
- spaces**
- innovation**
- model**
- important**
- designed**
- practices**
- commission**
- established**
- datasets**
- research**
- trade-offs**
- policy**
- openness**
- recommend**
- personal**
- assembly**
- essential**
- benefits**
- shared**
- economic**
- approach**
- human**
- cultural**
- preparation**
- community**
- internet**
- especially**
- linguistic**
- following**
- encryption**
- humanitarian**
- interests**
- without**
- include**
- justice**
- often**
- communities**
- information**
- ideas**
- contexts**
- rules**
- building**
- balance**
- public**
- global**
- contacts**
- provided**
- sectors**
- breaching**
- included**
- social**
- transparency**
- implementation**
- challenges**
- address**
- accountability**
- between**
- resolve**
- compilation**
- specific**
- clear**
- responses**
- issues**
- used**
- among**
- consent**
- working**
- levels**
- nuances**
- consider**
- swap**
- free**
- tools**
- additional**
- fundamental**
- local**
- flow**
- group**
- trust**
- health**
- digital**
- related**
- sharing**
- privacy**
- proposed**
- rights**
- raise**
- frameworks**
- protection**
- systems**
- observer**
- sovereignty**
- submitted**
- access**
- need**
- equity**
- enable**
- often**
- communities**
- information**
- ideas**
- contexts**
- rules**
- building**
- balance**
- public**
- global**
- contacts**
- provided**
- sectors**
- breaching**
- included**
- social**
- transparency**
- implementation**
- challenges**
- address**
- accountability**
- between**
- resolve**
- compilation**
- specific**
- clear**
- responses**
- issues**
- used**
- among**
- consent**
- working**
- levels**
- nuances**
- consider**
- swap**
- free**
- tools**
- additional**
- fundamental**
- local**
- flow**
- group**
- trust**
- health**
- digital**
- related**
- sharing**
- privacy**
- proposed**
- rights**
- raise**
- frameworks**
- protection**
- systems**
- observer**
- sovereignty**
- submitted**
- access**
- need**
- equity**
- enable**
- often**
- communities**
- information**
- ideas**
- contexts**
- rules**
- building**
- balance**
- public**
- global**
- contacts**
- provided**
- sectors**
- breaching**
- included**
- social**
- transparency**
- implementation**
- challenges**
- address**
- accountability**
- between**
- resolve**
- compilation**
- specific**
- clear**
- responses**
- issues**
- used**
- among**
- consent**
- working**
- levels**
- nuances**
- consider**
- swap**
- free**
- tools**
- additional**
- fundamental**
- local**
- flow**
- group**
- trust**
- health**
- digital**
- related**
- sharing**
- privacy**
- proposed**
- rights**
- raise**
- frameworks**
- protection**
- systems**
- observer**
- sovereignty**
- submitted**
- access**
- need**
- equity**
- enable**
- often**
- communities**
- information**
- ideas**
- contexts**
- rules**
- building**
- balance**
- public**
- global**
- contacts**
- provided**
- sectors**
- breaching**
- included**
- social**
- transparency**
- implementation**
- challenges**
- address**
- accountability**
- between**
- resolve**
- compilation**
- specific**
- clear**
- responses**
- issues**
- used**
- among**
- consent**
- working**
- levels**
- nuances**
- consider**
- swap**
- free**
- tools**
- additional**
- fundamental**
- local**
- flow**
- group**
- trust**
- health**
- digital**
- related**
- sharing**
- privacy**
- proposed**
- rights**
- raise**
- frameworks**
- protection**
- systems**
- observer**
- sovereignty**
- submitted**
- access**
- need**
- equity**
- enable**
- often**
- communities**
- information**
- ideas**
- contexts**
- rules**
- building**
- balance**
- public**
- global**
- contacts**
- provided**
- sectors**
- breaching**
- included**
- social**
- transparency**
- implementation**
- challenges**
- address**
- accountability**
- between**
- resolve**
- compilation**

Track 1 - Top 20 words:

- 45

13. Responses
14. Relevant
15. Balance
16. Rights
17. Sharing
18. Trust
19. Innovation
20. Accountability

Key Insights:

The prominence of terms such as “data,” “governance,” “principles,” “rights,” “trust,” and “accountability” signals that submissions from Track 1 converge around the need for a normative foundation anchored in human rights and public interest.

Submissions consistently emphasize that legitimacy depends on embedding “privacy,” “security,” and “transparency” into governance frameworks, reflecting a shared concern with maintaining trust in increasingly data-driven societies.

On the other hand, the recurrence of terms such as “development,” “innovation,” and “sharing” illustrates that these principles are not viewed as constraints alone but also as enablers of equitable growth and scientific progress.

This duality is reinforced by the frequent use of terms such as “balance,” “context,” and “relevant,” which signal a shared rejection of a one-size fits all approach. Instead, submissions advocate for sector-specific models, particularly for high-risk domains:

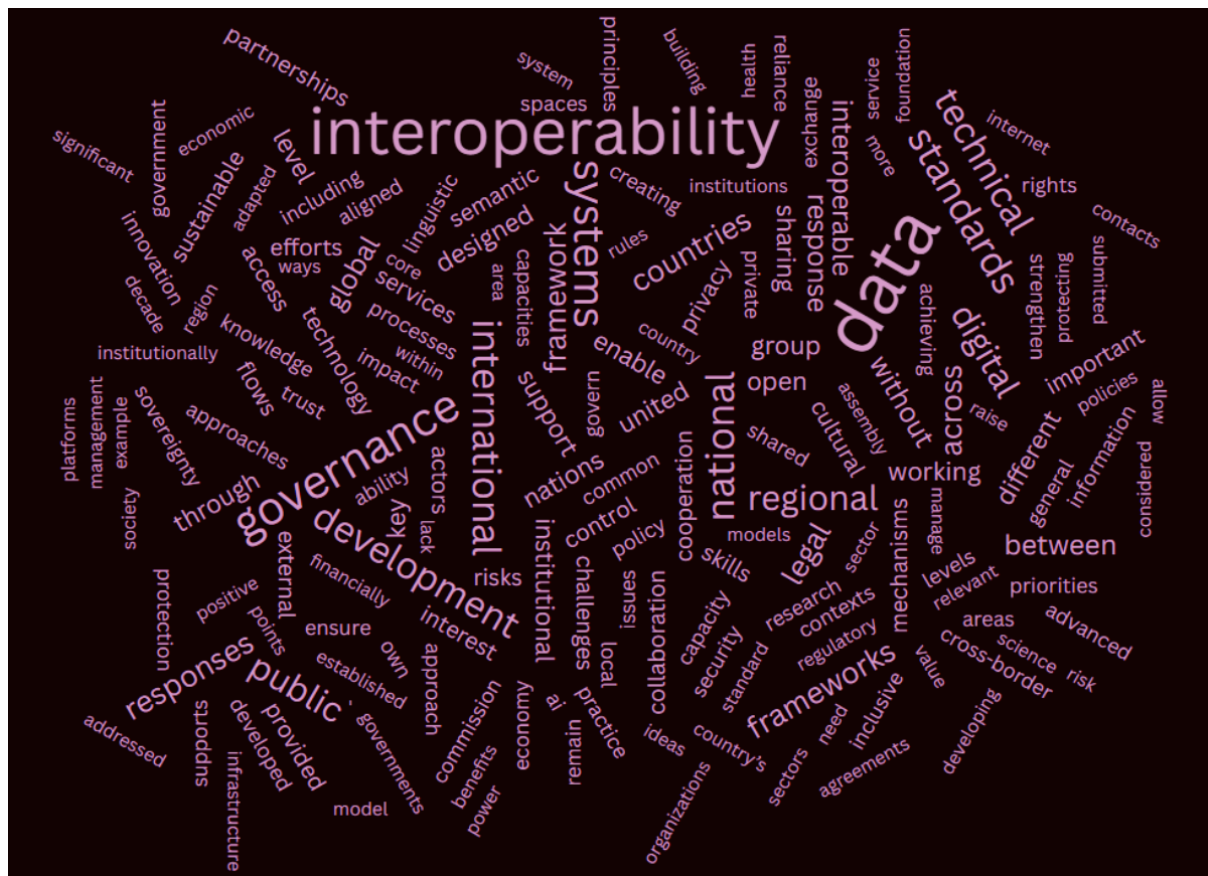
- **Health and genomics:** Where sensitive data must be balanced with public health imperatives.
- **Humanitarian action:** In the context of humanitarian crisis and the deployment of aids, open data can be weaponized, requiring controlled sharing and proportional limitations.
- **Environmental governance:** The governance of environmental and agricultural data must address power asymmetries between smallholders farmers and large businesses, to protect local communities from data extractivism and colonialism.
- **Artificial Intelligence (AI):** Requires stricter tracking of the provenance of data and the establishment of algorithm accountability to mitigate collective harms derived from AI.

Despite this convergence, significant divergences emerge in how these values should be operationalized. Tensions between “access” and sovereignty are reflected in opposing positions on cross-border data flows, with actors prompting open and trade-oriented frameworks while others emphasize data localization and state control. Similarly, the coexistence of “rights,” “equity,” and “fair” points to differing interpretations of rights-based governance between Western

individual-centric models, focused on consent and privacy and collective approaches emphasizing indigenous and community data rights. Finally, there is also a tension between “innovation” and “regulation,” as rapid technological advancements challenge the capacity of existing frameworks to adapt.

Submissions propose mechanisms such as federated governance models, allowing data to remain locally stored while enabling controlled sharing. Meanwhile data trusts and community consent models address collective rights benefit-sharing. Overall, submissions from Track 1 reveals a high degree of normative alignment but also underlines that a challenge remains in translating shared principles into adaptable and context-sensitive governance architectures.

Track 2: Supporting Interoperability Between National, Regional and International Systems



Number of Submissions: 64

Track 2 - Top 20 words:

1. Interoperability
2. Data
3. Governance
4. Systems
5. International
6. Standards
7. Technical
8. Frameworks
9. Development
10. Public
11. Regional
12. National
13. Sharing
14. Privacy
15. Capacity
16. Collaboration

- 17. Cross-border
- 18. Institutions
- 19. Open
- 20. Legal

Key Insights:

The vocabulary of Track 2, dominated by “interoperability”, “systems”, “standards”, “technical” and “frameworks” reflects a shift from normative principles to the practical and infrastructural conditions required to make data governance operational. Submissions converge on the idea that interoperability is a multi-layered challenge, requiring alignment at the technical level but also across semantic, organizational and legal dimensions. This is illustrated by the simultaneous presence of terms such as “technical”, “legal”, “privacy” and “institutions”, which signal that effective interoperability depends on coordinated governance across multiple layers. The frequent use of “international”, “cross-border” and “collaboration” highlights the inherently transnational nature of interoperability, while “national” and “regional” point the need for alignment across different governance scales.

The analysis of the submissions reinforce this convergence through the emphasis on establishing a minimal core of open, non-proprietary standards, combined with contextual flexibility to reflect linguistic, cultural and policy differences. This multi-layered approach is particularly visible in sectoral applications :

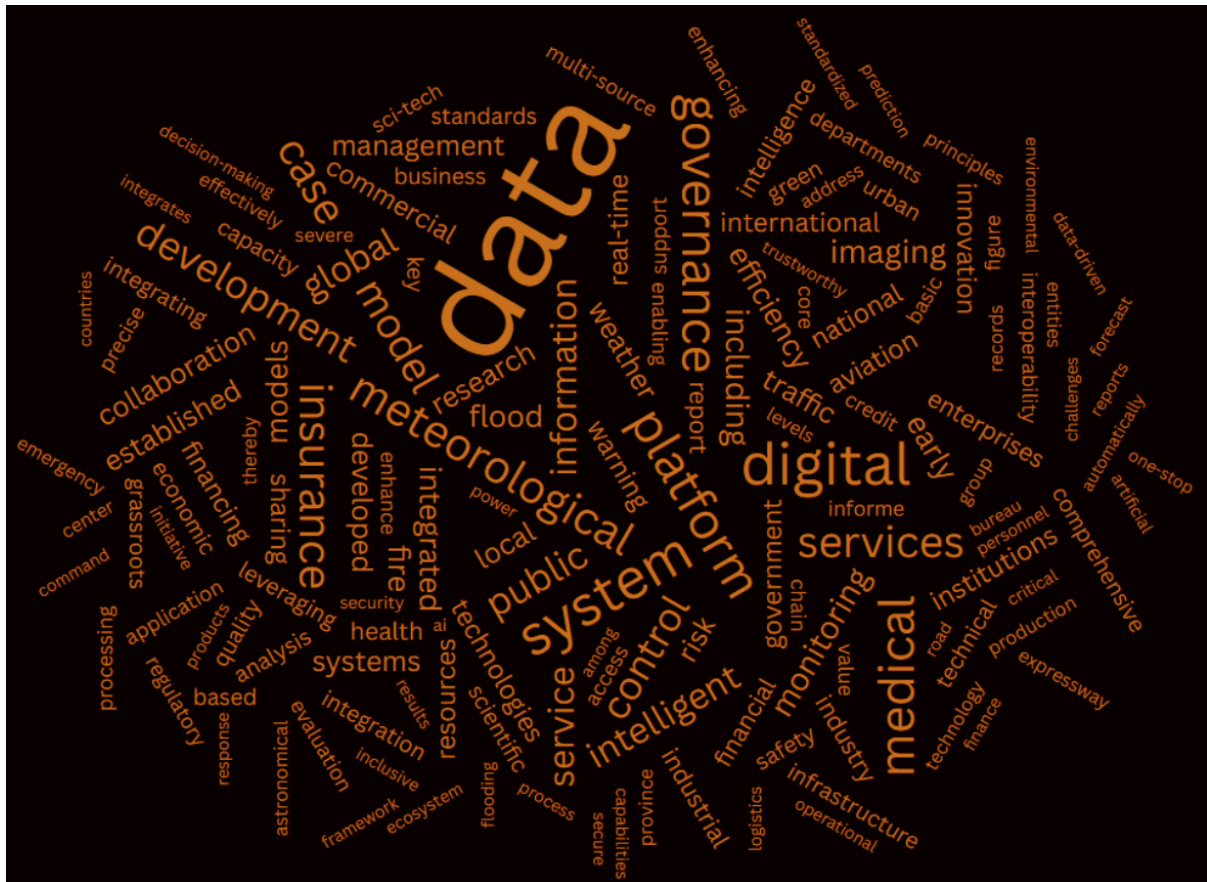
- **Public Service & Infrastructure:** Interoperability facilitates social protection systems and digital identity frameworks.
- **Health:** Real-time sharing of health data and coordinated pandemic responses are crucial needs for interoperable data systems in the health sector.
- **Environment:** Cross-border data exchanges are necessary for disaster risk mitigation, early warning systems and transboundary resource management.
- **Economic Development:** Reduce barriers for Small and Medium Enterprises (SMEs) by integrating supply chains and fostering inclusive digital inclusion.
- **Research:** Improves the quality of official statistics by linking data sources and open science infrastructures.

However, the vocabulary also translates to persistent challenges. Terms such as “systems” and “standards” coexist with indications of fragmentation, especially between syntactic and semantic interoperability. Institutional fragmentation is another key issue, with overlapping mandates and limited governance capacity undermining coordination.

Capacity building also emerges as a central theme, with “development” and “capacity” reflecting concerns that lack of infrastructure, skills and financial resources in developing countries, limiting

their ability to implement interoperable systems. It creates a risk of deepening global inequalities. Divergences are also apparent in the area of legal interoperability, as some actors advocate for harmonized frameworks, others warn that harmonization may undermine local priorities and policy autonomy. Similarly, tensions between interoperability and sovereignty persist. States seek to maintain control over data while still desiring to participate in the global system. Overall, Track 2 demonstrates a strong consensus on the necessity to push interoperability as an enabling condition for data governance. However, the submissions highlight that achieving this objective requires navigating complex technical, institutional and political trade-offs.

Track 3: Sharing the Benefits of Data



Number of Submissions: 58

Track 3 - Top 20 words:

1. Data
2. Platform
3. System
4. Governance
5. Digital
6. Services
7. Medical
8. Insurance
9. Meteorological
10. Information
11. Control
12. Monitoring
13. International
14. Public
15. Model
16. Management

- 17. Development
- 18. Innovation
- 19. Infrastructure
- 20. Standards

Key Insights:

Track 3 is distinct by its focus on the tangible outcomes of data governance, as reflected by the prominence of terms such as “platform”, “services”, “infrastructure”, or sector-specific references like “medical”, “insurance” and “meteorological”. It indicated that submissions are primarily concerned with how data systems generate value across different domains, from healthcare, public administration to industry and environmental monitoring. Words such as “innovation”, “development” and “management”, reinforce the perception of data as a key economic resource and a driver for productivity, market creation and digital transformation. At the same time, the presence of “control”, “monitoring” and “public”, suggests that governance is central to ensure that these benefits are realized in ways that serve the public interest.

The submissions reveal a fundamental divergence in how the benefits of data are conceptualized. On one hand, a political economy perspective emphasizes data sovereignty, market efficiency and the risks of value concentration among dominant platforms and hyperscalers. On the other hand, a data justice perspective stresses the need to redress structural inequalities and highlight issues such as data colonialism, the marginalization of developing countries and the importance of empowering indigenous communities to govern their own data. This tension is reflected in discussions on benefit distribution across the data life cycle, where control over infrastructure and analytical capacity often determines who captures value. Developing countries are frequently positioned as providers of raw data and lack the technical capacity to extract higher value insights.

Important gaps remain to capture the quantitative value and distribution of the benefits of data-sharing. It includes the absence of robust methodologies to measure non-monetary and intangible benefits, as well as the need to map how benefits are distributed at local and subnational levels. Capacity-building and infrastructure development therefore emerge as critical enablers through digital public goods, localized cloud infrastructure and community-based data institutions as key mechanisms to ensure equitable access and participation. However, tensions persist between open access mandates and intellectual property regimes. There is a broad agreement that standards and openness can expand participation but disagreements remain over how to balance data openness with sovereignty, investment incentives and innovation. Environmental considerations also surface with calls to better account for the energy and resource footprint of data infrastructures. Overall, Track 3 highlights that the main challenge is not only generating value from data, but also ensuring that this value is fairly distributed, sustainable and inclusive.

Track 4: Secure and Trusted Cross-Border Data Flows Relevant For Development



Number of Submissions: 62

Track 4 - Top 20 words:

1. Data
2. Governance
3. Flows
4. Cross-border
5. International
6. Sharing
7. Trust
8. Countries
9. Development
10. Mechanisms
11. Standards
12. Privacy
13. Protection
14. Frameworks
15. Access
16. Secure
17. Track

- 18. Including
- 19. Response
- 20. Regulation

Key Insights:

The vocabulary of Track 4 is mainly centered on “flows”, “cross-border”, “mechanism”, “standards”, “protection” and “secure”, reflecting a strong focus on the governance of international data exchanges. Submissions converge on the idea that cross-border data flows are essential for economic development, innovation and global cooperation as indicated by the presence of “development”, “sharing” and “access”. Additionally, the prominence of “trust”, “privacy” and “regulation” underlines a shared recognition that data flows must be underpinned by robust safeguards to ensure legitimacy and security. The frequent references to “countries”, “international” and “agreements” also highlight the geopolitical dimensions of this track, where governance is shaped by competing legal frameworks, trade regimes and national interests.

The submissions reveal two competing approaches to cross-border data governance. On the one hand, data liberalization promotes the Data Free Flow with Trust (DFFT) framework to facilitate trade and innovation. On the other hand, countries protective of their sovereignty call for data localization and domestic control as tools protecting against foreign surveillance, support local industry and address structural inequalities. These tensions are exacerbated by broader asymmetries including the “raw data trap”, where developing countries export raw data but lack the capacity to generate higher-value outputs. It led to calls for rights-based approaches incorporating collective and indigenous rights, as well as mechanisms to redistribute value and redress power imbalances.

In terms of implementation, submissions highlight a range of practical tools to reconcile competing priorities. Data intermediaries such as data trusts and data spaces are proposed to enable controlled sharing while preserving sovereignty. Privacy-Enhancing Technologies (PETs) are also presented as key enablers to secure data exchange without exposing sensitive information, including federated learning and encryption. Contractual and certification mechanisms, such as Standard Contractual Clauses (SCC) and cross-border privacy rules provide additional layers of assurance for the private sector. Overall, Track 4 underscores the persistent political and economic divides in the digital space despite a pragmatic effort to operationalize cross-border data flows in ways that balance openness, security and sovereignty.

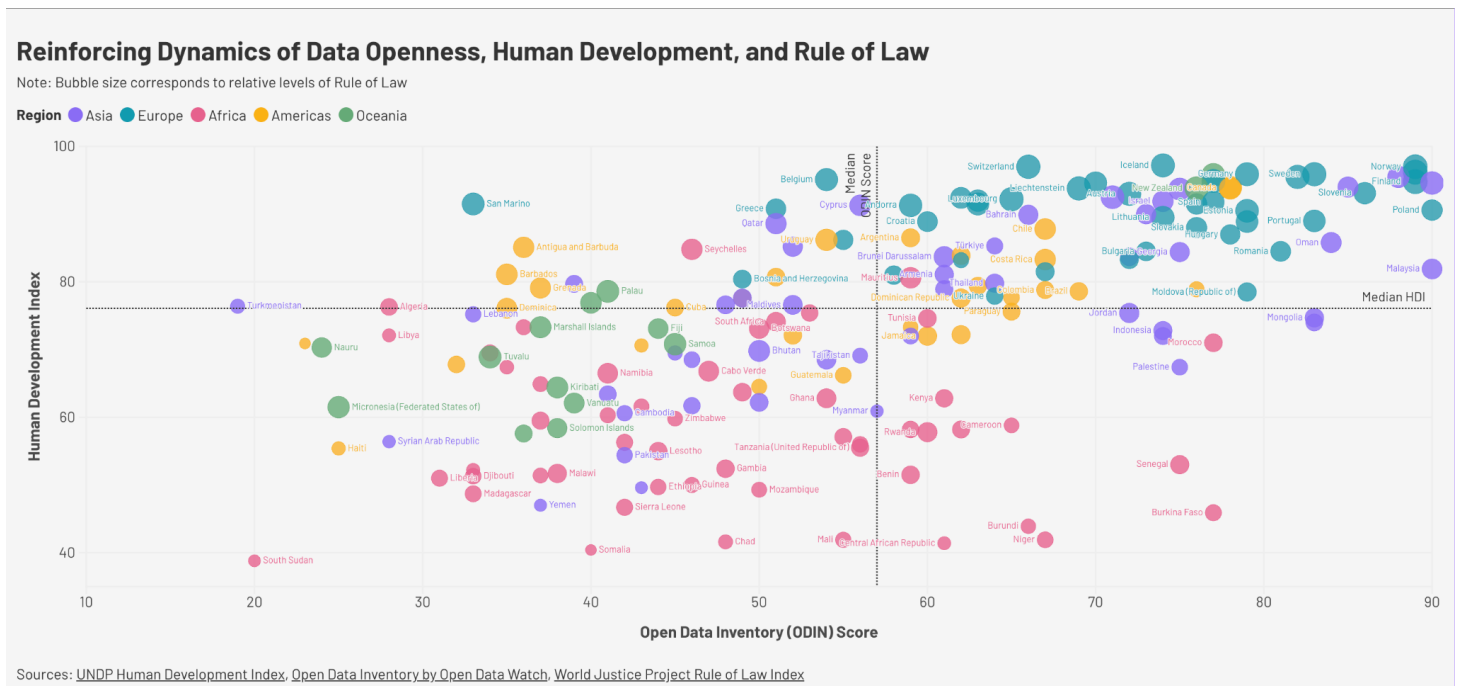
Common Ground Between Interoperability and Cross-Border Data Flows :

An analysis of the submissions show how Tracks 2 and 4 are closely interconnected, as they share a common focus on enabling data exchange across jurisdictions and systems. This is reflected in overlapping vocabulary such as “standards”, “frameworks”, “sharing”, “privacy” and “trust”. It points out a shared understanding that interoperability and cross-border data flows are mutually reinforcing dimensions of data governance. Submissions in both tracks emphasize interoperability as a prerequisite for effective cross-border data flows. Meanwhile, cross-border governance provides the legal and institutional context within which interoperable standards operate. Both tracks also converge on the importance of safeguards, with a strong emphasis on security, privacy and trust as a

condition for sustainable data exchange.

At the same time, the two tracks face similar tensions and challenges. The prominence of terms such as “national” and “control” reflects the ongoing struggle to balance domestic sovereignty with global integration. Fragmentation, whether technical, institutional or legal, emerges as a shared constraint, as well as the asymmetries of capacities between developed economies and low income countries. Both tracks also highlight similar implementation mechanisms, including federated data architectures, the deployment of Privacy-Enhancing Technologies and standardized contractual tools to bridge the gap between openness and control. Taken together, Tracks 2 and 4 illustrate that technical and regulatory dimensions of data governance are deeply intertwined. Achieving effective global data exchange therefore requires coordinated solutions that address both infrastructural and political constraints.

6.2 Data Openness, Human Development, and Rule of Law



This scatter plot highlights how levels of data openness (as indicated by the Open Data Inventory (ODIN) scores), human development (as indicated by the Human Development Index (HDI)), and rule of law (as indicated by the World Justice Project Rule of Law Index) tend to co-vary across countries worldwide.¹⁶⁰ While the relationship is not uniform, a general positive correlation emerges in which countries with higher levels of data openness tend to also exhibit higher levels of human development and stronger rule of law.

At the same time, the distribution of countries across the scatter plot shows that these relationships are neither linear nor deterministic. Countries with similar levels of data openness may exhibit different development outcomes, and vice versa, which suggests that data openness interacts with broader institutional, economic, and governance conditions rather than operating as a standalone driver.

This variation is also visible across regions. A number of European nations cluster in the upper-right quadrant, combining relatively high levels of data openness, human development, and rule of law. Countries in Asia and the Americas are more distributed. Across Africa, many countries are concentrated in the lower half of the scatter plot, though with variation across all three dimensions. Rather than showing a single trajectory, the variation observed across regions illustrates that there are multiple pathways through which countries engage with data governance. The fact that a large

¹⁶⁰ Access interactive scatter plot here: <https://public.flourish.studio/visualisation/28167748/>. For datasets, see “Open Data Inventory—Global Index of Open Data - Open Data Inventory,” opendatawatch.com, 2026, odin.opendatawatch.com/data; United Nations Development Programme, “Human Development Index,” United Nations, 2024, hdr.undp.org/data-center/human-development-index#/indicies/HDI; and World Bank Data360, “Rule of Law Index” 2025, data360.worldbank.org/en/dataset/WJP_ROL.

number of countries cluster around the mid-range levels of data openness and human development suggests that there is a practical trade-off involved in expanding access to data while strengthening institutional capacity and managing governance constraints.

Several outliers, however, deserve particular attention. In some contexts, particularly among a subset of African countries, relatively high levels of data openness coexist with lower human development outcomes, suggesting that investment in data infrastructure has not yet translated into broader social and economic gains. Conversely, other countries exhibit the opposite pattern, combining comparatively high human development with more limited data openness, implying that development gains can, in some cases, emerge without more open data ecosystems. In other cases, resource-driven growth can further decouple development outcomes from open governance practices. These patterns underscore that while the overall relationship between data openness, development, and rule of law is generally positive, it is not necessarily set in stone. Factors such as national context, resource wealth, and governance models can shape how these dimensions interact over time.

7. REFERENCES

7.1 Bibliography

A note on the use of generative AI: Elements of this report were developed with assistance from AI tools, namely for language clarity, outline structuring, and formatting of references. All content has been reviewed and edited by the authors.

Overview

African Union. *African Digital Compact (ADC)*. African Union Commission, August 9, 2024. https://au.int/sites/default/files/documents/44005-doc-AU_Digital_Compact_V4.pdf. Accessed November 28, 2025.

African Union Commission. *African Union Data Policy Framework*. Addis Ababa: African Union, February 2022, <https://au.int/sites/default/files/documents/42078-doc-DATA-POLICY-FRAMEWORKS-2024-ENG-V2.pdf>. Accessed November 28, 2025.

African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention). adopted June 27, 2014. https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf. Accessed November 28, 2025.

APEC Cross-Border Privacy Rules (CBPR) System, updated as of November 2019. <https://cbprs.org/wp-content/uploads/2019/11/4.-CBPR-Policies-Rules-and-Guidelines-Revision-3-16-updated-1709-2019.pdf>. Accessed November 28, 2025.

ASEAN Secretariat; Boston Consulting Group; Australian Government (Australia for ASEAN Futures Economic and Connectivity). *Study on the ASEAN Digital Economy Framework Agreement (DEFA), Public Version 2.0*. November 8, 2024. https://asean.org/wp-content/uploads/2024/11/DEFA-Report-public-summary-expanded_Final_25112024.pdf. Accessed November 28, 2025.

Beijing Post. “China’s Digital Landscape: A Comprehensive Overview of ‘Digital China’ Initiatives.” *Beijing Post*, November 21, 2025. <https://beijingpost.com/china-s-digital-landscape-a-comprehensive-overview-of-digital-china-initiatives>. Accessed November 28, 2025.

Benfeldt, Olivia, John Stouby Persson, and Sabine Madsen. *Data Governance as a Collective Action Problem*. *Information Systems Frontiers*, vol. 22, no. 2 (2020): 299–313. <https://doi.org/10.1007/s10796-019-09923-z>. Accessed November 28, 2025.

Bentotahewa, Vibhushinie, Chaminda Hewage and Jason Williams. “The Normative Power of the GDPR: A Case Study of Data Protection Laws of South Asian Countries,” *SN Computer Science* 3, no. 3 (2022): 183, <https://doi.org/10.1007/s42979-022-01079-z>. Accessed November 29, 2025.

- Brazil. *Lei No. 13.709, de 14 de Agosto de 2018*, amended by *Lei No. 13.853/2019* (LGPD).
https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Accessed November 28, 2025.
- Canada. Personal Information Protection and Electronic Documents Act (PIPEDA), S.C. 2000, c. 5.
<https://laws-lois.justice.gc.ca/eng/acts/P-8.6/>. Accessed November 28, 2025.
- China. Cybersecurity Law (CSL) of the People's Republic of China, adopted November 7, 2016.
<https://www.lawinfochina.com/Display.aspx?Id=22826&Lib=law&LookType=3>. Accessed November 28, 2025.
- China. Data Security Law (DSL) of the People's Republic of China, adopted June 10, 2021.
https://en.spp.gov.cn/2021-06/10/c_948426_2.htm. Accessed November 28, 2025.
- Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP).
<https://www.dfat.gov.au/trade/agreements/in-force/cptpp/comprehensive-and-progressive-agreement-for-trans-pacific-partnership>. Accessed November 28, 2025.
- Crowell & Moring LLP. "Latin American Data Privacy." *Crowell & Moring Insights*, January 28, 2025.
<https://www.crowell.com/en/insights/publications/latin-american-data-privacy>. Accessed November 28, 2025.
- Digital Economy Partnership Agreement (DEPA).
<https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-in-force/digital-economy-partnership-agreement-depa/overview>. Accessed November 28, 2025.
- European Union. *Data Act: Regulation (EU) 2023/2854*.
<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R2854>. Accessed November 28, 2025.
- European Union. *Data Governance Act: Regulation (EU) 2022/868*.
<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0868>. Accessed November 28, 2025.
- European Union. *General Data Protection Regulation (GDPR): Regulation (EU) 2016/679*.
<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679>. Accessed November 28, 2025.
- Ferracane, Martina Francesca. Data Governance Models and Geopolitics: Insights from the Indo-Pacific Region. Policy Briefs, 2022/48, Global Governance Programme. European University Institute, 2022.
<https://cadmus.eui.eu/server/api/core/bitstreams/d76f633f-0ab8-5eb5-a876-8984917dae6e/content>. Accessed November 29, 2025.
- Gulf News Report. "How AI, Data Sovereignty and Open Source Are Redefining Leadership in the Middle East." *Gulf News*, February 11, 2025.

<https://gulfnews.com/business/how-ai-data-sovereignty-and-open-source-are-redefining-leadership-in-the-middle-east-1.500033816>. Accessed November 28, 2025.

Hassani, Hossein, Xu Huang, and Steve MacFeely. "Mapping the Evolution of Data Governance Scientific Research." *Data & Policy* 7 (2025): e51. <https://doi.org/10.1017/dap.2025.10014>. Accessed November 29, 2025.

India. Digital Personal Data Protection Act, 2023, No. 22 of 2023, enacted August 11, 2023. <https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf>. Accessed November 29, 2025.

International Telecommunication Union. Collaborative Regulation: Accelerating Nigeria's Digital Transformation. 2023. <https://digitalregulation.org/wp-content/uploads/d-pref-them.33-2023-pdf-e.pdf>. Accessed November 29, 2025.

International Telecommunication Union. Collaborative Regulation for Digital Transformation in Kenya: A Country Review. 2023. https://digitalregulation.org/wp-content/uploads/D-PREF-THEM.32_Kenya-2023-PDF-E.pdf. Accessed November 29, 2025.

Jiang, Christine J., and Sabrina Martin. *The Geopolitics of Data Governance Research Report Part I: Data Governance Regimes*. Oxford Insights, May 2020. https://oxfordinsights.com/wp-content/uploads/2024/08/The-Geopolitics-of-Data-Governance_Oxford_insights_Master.pdf. Accessed November 28, 2025.

ONDC (Open Network for Digital Commerce). *ONDC Network Policies and Documentation*. 2024. <https://www.ondc.org/rfp/>. Accessed November 28, 2025.

South Africa. Protection of Personal Information Act (POPIA), Act 4 of 2013. <https://www.gov.za/documents/protection-personal-information-act>. Accessed November 28, 2025.

South Korea. Personal Information Protection Act (PIPA), Act No. 10465. https://elaw.klri.re.kr/eng_service/lawView.do?hseq=62389&lang=ENG. Accessed November 28, 2025.

United Nations. *Global Digital Compact*. United Nations, 2024. https://www.un.org/global-digital-compact/sites/default/files/2024-09/Global%20Digital%20Compact%20-%20English_0.pdf. Accessed November 28, 2025.

United Nations Conference on Trade and Development (UNCTAD). Digital Economy Report 2021: Cross-border Data Flows and Development — For Whom the Data Flow? Geneva: UNCTAD, 2021. https://unctad.org/system/files/official-document/der2021_en.pdf. Accessed November 29, 2025.

United Nations Conference on Trade and Development (UNCTAD). Summary of Adoption of E-Commerce Legislation Worldwide. UNCTAD Global Cyberlaw Tracker. <https://unctad.org/topic/ecommerce-and-digital-economy/ecommerce-law-reform/summary-adoption-e-commerce-legislation-worldwide>. Accessed November 29, 2025.

United States. Children's Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501–6506 (1998). <https://www.ftc.gov/legal-library/browse/statutes/childrens-online-privacy-protection-act>. Accessed November 28, 2025.

United States. Gramm–Leach–Bliley Act (Financial Services Modernization Act of 1999), Pub. L. No. 106-102, 113 Stat. 1338 (1999). <https://www.govinfo.gov/content/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf>. Accessed November 28, 2025.

United States. Health Insurance Portability and Accountability Act (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (1996). <https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf>. Accessed November 28, 2025.

United States–Mexico–Canada Agreement (USMCA), signed November 30, 2018; entered into force July 1, 2020. <https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement>. Accessed November 28, 2025.

Literature Review

Aaltonen, Aleksii et al., “What Is Missing from Research on Data in Information Systems? Insights from the Inaugural Workshop on Data Research.” *Communications of the Association for Information Systems* 53 (2023): 475–90. <https://doi.org/10.17705/1CAIS.05320>.

Alaimo, Cristina, and Jannis Kallinikos. “Organizations Decentered: Data Objects, Technology and Knowledge.” *Organization Science* 33, no. 1 (2022): 19–37. <https://doi.org/10.1287/orsc.2021.1552>.

Ishkhanyan, Artur. “The Sovereignty–Internationalism Paradox in AI Governance: Digital Federalism and Global Algorithmic Control,” *Discover Artificial Intelligence* 5 (2025): 123. <https://doi.org/10.1007/s44163-025-00374-x>.

Jungherr, Andreas. “Artificial Intelligence and Democracy: A Conceptual Framework.” *Social Media + Society* 9, no. 3 (2023): 1–14. <https://doi.org/10.1177/20563051231186353>.

Koutroumpis, Pantelis, Aija Leiponen, and Leonard D. Thomas. “Markets for Data.” *Industrial and Corporate Change* 29, no. 3 (2020): 645–60.

Kuzio, Jacqueline, et al., “Building Better Global Data Governance.” *Data & Policy* 4 (2022): e24. <https://doi.org/10.1017/dap.2022.17>.

Kwet, Michael. "Digital Colonialism and Infrastructure-as-Debt." *Frontiers in African Digital Research* 9 (2021): 66–72. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4004594.

Marcucci, Sara, et al. "Informing the Global Data Future: Benchmarking Data Governance Frameworks." *Data & Policy* 5 (January 2023). <https://doi.org/10.1017/dap.2023.24>.

Organisation for Economic Co-operation and Development (OECD). *Going Digital: Guide to Data Governance Policy Making*. Paris: OECD Publishing, 2022.

Taylor, Linnet. "What Is Data Justice? The Case for Connecting Digital Rights and Freedoms Globally." *Big Data & Society* 4, no. 2 (2017): 1–14. <https://doi.org/10.1177/2053951717736335>.

Roguski, Piotr. "Layered Sovereignty: Adjusting Traditional Notions of Sovereignty to a Digital Environment." In *11th International Conference on Cyber Conflict: CyCon*, edited by Tomáš Minárik, et al., 347–359. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2019.

United Nations Conference on Trade and Development (UNCTAD). *Data for Development*. Geneva: United Nations Conference on Trade and Development, 2024.

Analytical Brief

Adam Clark, *Research Briefing - Digital Sovereignty* (London, UK: House of Commons Library, 2026), <https://researchbriefings.files.parliament.uk/documents/CBP-10547/CBP-10547.pdf>.

Brooke Tanner et al., *Is AI Sovereignty Possible? Balancing Autonomy and Interdependence* (Washington, DC: Brookings Institution, February 2026), https://www.brookings.edu/wp-content/uploads/2026/02/20260217_AI_sovereignty_final.pdf.

Daskal, Jennifer. "The un-territoriality of data." *Yale IJ* 125 (2015): 326.

Data Sovereignty: From the Digital Silk Road to the Return of the State edited by Anupam CHANDER and Haochen SUN. Oxford: Oxford University Press, 2023.

Felix von Scherenberg, Moritz Hellmeier, and Boris Otto, "Data Sovereignty in Information Systems," *Electronic Markets* 34, no. 1 (2024): 15, <https://doi.org/10.1007/s12525-024-00693-4>.

González Morales, Luis Gerardo, and Tom Orrell. "Data interoperability: A practitioner's guide to joining up data in the development sector." (2018), <https://unstats.un.org/wiki/spaces/InteropGuide/pages/36143964/Home>.

Google Trends, "Search interest for 'data sovereignty,' 'digital sovereignty,' and related terms," accessed April 12, 2026, <https://trends.google.com>.

Gray, John. *Al Qaeda and What It Means to Be Modern*. New York: The New Press, 2003.

Hassani, Hossein, Xu Huang, and Steve MacFeely. "Mapping the Evolution of Data Governance Scientific Research." *Data & Policy* 7 (2025): e51. <https://doi.org/10.1017/dap.2025.10014>.

Hummel, Patrik, Matthias Braun, Max Tretter, and Peter Dabrock. "Data sovereignty: A review." *Big Data & Society* 8, no. 1 (2021): 2053951720982012, <https://doi.org/10.1177/2053951720982012>.

Interoperability of Data Governance Regimes: Challenges for Digital Trade Policy, Bacchus J, Borchert I, Marita-Jaeger M, Ruiz Diaz J, 2024, <https://citp.ac.uk/publications/interoperability-of-data-governance-regimes-challenges-for-digital-trade-policy>

James Gorgen, "How Trump's Data Regulation Crackdown Undermines Digital Sovereignty," Tech Policy Press, March 12, 2026, <https://www.techpolicy.press/how-trumps-data-regulation-crackdown-undermines-digital-sovereignty/>.

Nagan, Winston P., and Aitza M. Haddad. "Sovereignty in theory and practice." *San Diego Int'l LJ* 13 (2011): 429.

Sean Mullin and Jaxson Khan, *Sovereignty by Design: Strategic Options for Canadian AI Sovereignty* (Toronto: Munk School of Global Affairs and Public Policy, 2026), <https://aicompetitiveness.ca/assets/Sovereign-by-Design-Full-Report-2026.pdf>.

United Nations Conference on Trade and Development (UNCTAD). *Data Governance for Development Working Group: Submissions by Members and Observers*. 2025. Unpublished materials (accessed through the author's participation in the Working Group).

Thematic Articles

"From Policy to Public, from Public to Policy"

Alemany, Cecilia, Gurumurthy Anita, Chami Nandini, "Gender Equality in the Digital Economy: Emerging Issues," *Feminist Digital Justice* 1(2019). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3872572

Bengtsson, Linus, Xin Lu, Anna Thorson, Richard Garfield, and Johan Von Schreeb. "Improved Response to Disasters and Outbreaks by Tracking Population Movements With Mobile Phone Network Data: A Post-Earthquake Geospatial Study in Haiti." *PLoS Medicine* 8, no. 8 (August 30, 2011): e1001083. <https://doi.org/10.1371/journal.pmed.1001083>.

- Birkland, Thomas A. "Focusing Events, Mobilization, and Agenda Setting." *Journal of Public Policy* 18, no. 1 (1998): 53–74.
<http://www.jstor.org/stable/4007601>
- Blum, Sonja, and Johanna Kuhlmann. 2019. "Stories of How to Give or Take – towards a Typology of Social Policy Reform Narratives." *Policy and Society* 38 (3): 339–55.
<https://doi.org/10.1080/14494035.2019.1657607>
- Bucchi, Massimiano, and Brian Trench, eds. *Routledge Handbook of Public Communication of Science and Technology*. 3rd ed. London: Routledge, 2021.
- Cadwalladr, Carole and Emma Graham-Harrison, "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data". *The Guardian*, March 17, 2018.
<https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-u-s-election>
- Capstick, Stuart, Lorraine Whitmarsh, Wouter Poortinga, Nick Pidgeon, and Paul Upham. 2014. "International Trends in Public Perceptions of Climate Change over the Past Quarter Century." *Wiley Interdisciplinary Reviews: Climate Change* 6 (1): 35–61.
<https://doi.org/10.1002/wcc.321>.
- Dencik, Lina, Arne Hintz, Joanna Redden, and Emiliano Treré. 2019. "Exploring Data Justice: Conceptions, Applications and Directions." *Information, Communication & Society* 22, no. 7(2019): 873–81, <https://doi.org/10.1080/1369118X.2019.1606268>
- Dron, L, Kalatharan V, Gupta A et al. "Data capture and sharing in the COVID-19 pandemic: a cause for concern" *The Lancet Digital Health* 4, no. 10(2022): e748-e756
- Entman, R. M. (1993). "Framing: Toward clarification of a fractured paradigm". *Journal of Communication* 43, no. 4 (1993), 51–58. <https://doi.org/10.1111/j.1460-2466.1993.tb01304.x>
- McBeth MK, Jones MD and Shanahan EA, "The narrative policy framework", in (2018). *Theories of the Policy Process*, ed. M. Weible, C., & Sabatier, P.A. (Routledge, 2018)
<https://doi.org/10.4324/9780429494284>
- Mcclain, Coleen, Faverio Michelle, Anderson Monica, Park Eugenie, "How Americans View Data Privacy", *Pew Research Center*, October 18, 2023. Accessed April 7, 2026
https://www.pewresearch.org/wp-content/uploads/sites/20/2023/10/PI_2023.10.18_Data-Pri vacy_FINAL.pdf?_gl=1*8yonnn*_up*MQ..*_gs*MQ..&gclid=CjwKCAjwnN3OBhA8EiwAfpTYegGMM6k0_inOn5l5U5W_9d7AugYVrdpIXHT9rprSD2Mn419vg8OXjhoCW4oQAvD_BwE&gbraid=0AAAAA-ddO9F7BTNTcH5TwHdgl8Kq5ziO

McCombs, Maxwell E., and Donald L. Shaw. "The Agenda-Setting Function of Mass Media." *The Public Opinion Quarterly* 36, no. 2 (1972): 176–87. <http://www.jstor.org/stable/2747787>.

Milan, Stefania, & Treré Emiliano, "Big Data from the South(s): Beyond Data Universalism". *Television & New Media* 20, no. 4(2019), 319–335. <https://doi.org/10.1177/1527476419837739>

Nisbet, Matthew C., "Communicating Climate Change: Why Frames Matter for Public Engagement", *Environment: Science and Policy for Sustainable Development* 51, no. 2(2009): 12-23, <https://doi.org/10.3200/ENVT.51.2.12-23>

Nisbet, Matthew C., and Teresa Myers. 2007. "Trends: Twenty Years of Public Opinion about Global Warming." *The Public Opinion Quarterly* 71 (3): 444–70. <https://www.jstor.org/stable/4500386>.

Nisbet, Matthew C. "Framing Science: A New Paradigm in Public Engagement." In *Communicating Science*, 1st ed., 54–81. Rutledge, 2009. <https://doi.org/10.4324/9780203867631-10>.

Nisbet, Matthew C., and Dietram A. Scheufele. "What's Next for Science Communication? Promising Directions and lingering distractions" *American Journal of Botany* 96, no. 10 (2009): 1767–1778. <https://doi.org/10.3732/ajb.0900041>

Rughinis, C., Rughinis, R., Toma, S. and Vulpe, S.N. (2021). "From Social Netizens to Data Citizens: Variations of GDPR Awareness in 28 European Countries." *Computers Law & Security Review* 42(2021), <https://doi.org/10.1016/j.clsr.2021.105585>

Staunton C, Hannay E, John O, Johnson M, Kadam R, Sampath R, "The governance of personal data for COVID-19 response: perspective from the Access to COVID-19 Tools Accelerator". *BMJ Glob Health* 6 no. 5 (2021): e006095. doi: 10.1136/bmjgh-2021-006095

UNCTAD, *Digital Economy Report: Cross-border data flows and development: For whom the data flow*, (2021), 16-17; 107. Available here: https://unctad.org/system/files/official-document/der2021_en.pdf

"Whose Cloud, Whose Coffee?"

"Beyco." 2026. beyco.nl. 2026. <https://beyco.nl/>.

"Building Data Interoperability in Agriculture - Farm Foundation." 2023. Farm Foundation. October 16, 2023. <https://www.farmfoundation.org/projects/building-data-interoperability-in-agriculture/>.

"Coffee and Carbon in Colombia: Human Rights Concerns at the Intersection of Food Systems, Climate Change and Data-Based Technologies." 2024. FIAN International. [https://www.fian.org/files/is/htdocs/wp11102127_GNIAANVR7U/www/files/Coffee_Carbon_Markets_20240624_abfin\(2\).pdf](https://www.fian.org/files/is/htdocs/wp11102127_GNIAANVR7U/www/files/Coffee_Carbon_Markets_20240624_abfin(2).pdf).

- “Colombia Launches Traceability Platform in September.” 2024. Tridge. September 4, 2024.
<https://www.tridge.com/news/colombia-launches-traceability-platform-in-s-hfdoar>.
- “Data Governance Act | Shaping Europe’s Digital Future.” Digital-Strategy.ec.europa.eu. 2023.
<https://digital-strategy.ec.europa.eu/en/policies/data-governance-act>.
- “Digital Coffee Farmer: IoT Sensors and AI for Smarter Coffee Decisions.” 2025. Colombia One: News from Colombia and the World. December 19, 2025.
<https://colombiaone.com/2025/12/19/digital-coffee-farmer-iot-sensors-ai-coffee-farming/>.
- “Empowering Coffee Cooperatives with Digital Data Management: A Case Study on Carbon Insetting and Traceability Using the Beyco Platform in Colombia.” n.d. Solidaridad Network. Accessed April 13, 2026.
https://www.solidaridadnetwork.org/wp-content/uploads/2025/12/Empowering-Coffee-Cooperatives-with-Digital-Data-Management_Solidaridad.pdf.
- “Epistemic Justice | IPBES Secretariat.” 2024. IPBES Secretariat. 2024.
<https://www.ipbes.net/glossary-tag/epistemic-justice>. European Commission. 2023.
- Fakhri, Michael. “Report of the Special Rapporteur on the Right to Food, Michael Fakhri: Corporate Power and Human Rights in Food Systems.” UN.org, United Nations General Assembly, 21 July 2025, docs.un.org/en/A/80/213.
- GS1 Switzerland, “Digital Product Passport,”
<https://www.gs1.ch/en/products-services/digital-product-passport>.
- Hansberry, Cate. 2024. “Global DPI Models: Lessons from India, Brazil, and Beyond.” Atlantic Council. October 25, 2024.
<https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/global-dpi-models-lessons-from-india-brazil-and-beyond/>.
- Viladrich Beiroa, Oscar. 2025. “Digital Solutions for Smallholder Cooperatives under the European Union Deforestation Regulation: A Case Study in Ivory Coast.”
https://essay.utwente.nl/fileshare/file/109147/Oscar_Viladrich%20-%20Digital%20solutions%20for%20Smallholder%20Cooperatives%20under%20the%20EUDR.pdf.
- Wageningen University & Research. 2026. “Coffee Sector in Colombia: Statistics and Overview of the Value Chain.” Resiliencebv.com. November 2026.
https://resiliencebv.com/wp-content/uploads/2025/03/coffee_sector_in_colombia_statistics_and_overview-wageningen_university_and_research_686996.pdf.

“Strengthening Indigenous Data Sovereignty and Knowledge Co-Production”

Estabrooks, Carole A. "Reflections on Co-production as a Mode of Knowledge Production: Comment on 'Research Coproduction: An Underused Pathway to Impact.'"

European Union. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*. Official Journal of the European Union L119 (2016): 1–88. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>.

Global Indigenous Data Alliance. *Global Indigenous Data Alliance*. Accessed April 11, 2026. <https://www.gida-global.org/>.

Government of India, Ministry of Environment and Forests. *Community Biodiversity Registers: Guidelines for Documentation of Biodiversity at Local Level*. New Delhi: Government of India, 2009.

Indigenous Data Alliance. *Indigenous Data Alliance*. Accessed April 11, 2026.

Latulippe, Nicole, and Nicole Klenk. "Making Room and Moving Over: Knowledge Co-production, Indigenous Knowledge Sovereignty and the Politics of Global Environmental Change Decision-Making." *Current Opinion in Environmental Sustainability* 42 (2020): 7–14.

McCutchan, Sabrina. *Research Data Governance for Global Health: A Landscape Analysis*. Version 1.1. Durham, NC: Duke Global Health Institute, September 26, 2022.

Ministry of Culture of the Russian Federation. *Federal Register of Intangible Cultural Heritage Objects*. Moscow: Government of the Russian Federation, 2010. Accessed April 11, 2026.

Native Nations Institute. "Indigenous Data Sovereignty and Governance." Accessed April 11, 2026. <https://nni.arizona.edu/>.

Nelson, Amy Hawn. "Centering Community Involvement and Equity Across the Data Life Cycle." *Harvard Data Science Review*, no. Special Issue 2 (2021). <https://hdsr.mitpress.mit.edu/>.

People's Ecological Planning (PEP). *People's Ecological Planning: Community-Based Ecological and Development Approaches in India*. Accessed April 11, 2026. <https://www.sristi.org/>

Research Data Alliance International Indigenous Data Sovereignty Interest Group. *CARE Principles for Indigenous Data Governance*. Global Indigenous Data Alliance, 2019. <https://www.gida-global.org/care>.

Research Data Alliance International Indigenous Data Sovereignty Interest Group. *International Indigenous Data Sovereignty Interest Group*. Accessed April 11, 2026. <https://www.rd-alliance.org/groups/indigenous-data-sovereignty-ig>.

Sen, Bharati. "Indigenous Knowledge for Development: Bringing Research and Practice Together." *International Information & Library Review* 37, no. 4 (2005): 375–382.

Sharakhmatova, Victoria N. "Indigenous Knowledge Data Management Issues and Co-Production of Knowledge in Kamchatka." *Data Science Journal* 20, no. 1 (2021): 1–10.
<https://doi.org/10.5334/dsj-2021-XXX>.

U.S. Indigenous Data Sovereignty Network. *U.S. Indigenous Data Sovereignty Network*. Accessed April 11, 2026. <https://usindigenousdata.org/>.

United Nations Conference on Trade and Development (UNCTAD). "5th Meeting of the UN CSTD Multi-stakeholder Working Group on Data Governance at All Levels." Accessed April 11, 2026.
<https://unctad.org/meeting/5th-meeting-un-cstd-multi-stakeholder-working-group-data-governance-all-levels>.

"Embedding Human Rights and Data Justice in Health Data Governance"

Boulet, Pascale, Ellen 't Hoen, Katrina Perehudoff, Kaitlin Mara, and Ernest Tan. *Advanced Purchase Agreements for COVID-19 Vaccines: Analysis and Comments*. Brussels: The Left in the European Parliament, 2021.

European Union. *Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation)*. Official Journal of the European Union L 119 (2016): 1–88.

Framework Convention on Global Health (FCGH) Alliance. "Framework Convention on Global Health." Accessed April 11, 2026.

Lawrence O. Gostin, "Human Rights and the COVID-19 Pandemic." *Journal of the American Medical Association* 323, no. 24 (2020): 2470–2471. <https://doi.org/10.1001/jama.2020.6647>.

Holly, Louise. *Strengthening Health Data Governance: New Equity and Rights-Based Principles*.

Muscat, Danielle, Rachael Hinton, Don Nutbeam, Erin Kenney, Shyama Kuruvilla, and Zsuzsanna Jakab. "Universal Health Information Is Essential for Universal Health Coverage." *Family Medicine and Community Health* 11, no. 2 (2023).

Organisation for Economic Co-operation and Development (OECD). *Recommendation of the Council on Health Data Governance*. Paris: OECD, 2017.

Platformable. "Health Data Governance: An Overview." *Platformable*.

Perehudoff, Katrina, et al. "Improving Access to COVID-19 Vaccines: An Analysis of TRIPS Waiver Discourse Among WTO Members, Civil Society Organizations, and Pharmaceutical Industry Stakeholders." *Health and Human Rights Journal*, December 6, 2022.

Sander, Barrie, and Luca Belli. "COVID-19, Cyber Surveillance Normalization and Human Rights Law." *COVID-19 Symposium*.

Shaw, David, and T. Sekalala. *Health Data Justice: Building New Norms for Health Data Governance*.

Tiffin, Nick, and George LeFevre. *How to Use Relevant Data for Maximal Benefit with Minimal Risk: Digital Health Data Governance to Protect Vulnerable Populations in Low-Income and Middle-Income Countries*.

Transform Health Coalition. *Health Data Governance Principles*. 2020.
<https://transformhealthcoalition.org/areas-of-focus/health-data-governance/>

United Nations Economic and Social Council. *The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights*. UN Doc. E/CN.4/1985/4, 1984.

United Nations General Assembly. *International Covenant on Economic, Social and Cultural Rights (ICESCR)*. Adopted December 16, 1966. United Nations Treaty Series 993 (1976): 3.

United Nations General Assembly. *International Covenant on Economic, Social and Cultural Rights (ICESCR)*. Article 12(1). United Nations Treaty Series 993 (1976): 3.

Wang, Liang, Quanyi Wang, and George F. Gao. “Interpreting COVID-19 Data from China: A Call for Caution—Authors’ Reply.” *The Lancet Infectious Diseases*.

World Health Organization. *Ethics and Governance of Artificial Intelligence for Health: WHO Guidance (PDF)*. Geneva: World Health Organization.

World Health Organization. “International Health Regulations (IHR).” *World Health Organization*, accessed April 11, 2026.

World Health Organization. *Health Data Governance Summit: Summary Report*. Geneva: World Health Organization, 2021.

World Health Organization. *WHO Guidance on Ethics and Governance of Artificial Intelligence for Health*. Geneva: World Health Organization, 2021.