Submission to the UN CSTD Working Group on Data Governance

Track 2: Proposals to Support Interoperability Between National, Regional, and International Data Systems

22 August 2025

IT
for
Change

Submission to the UN CSTD Working Group on Data Governance

Track 2: Proposals to Support Interoperability Between National, Regional, and International Data Systems

22 August 2025

This input has been prepared by Anita Gurumurthy (member of the UN CSTD Working Group on Data Governance and Executive Director of IT for Change) with research support from team members, Amoha Sharma, Merrin Muhammed Ashraf, Nandini Chami, and Shobhit S.

The below submission includes answers to select questions shared by the co-facilitators for this track. Question numbers are indicated as per the numbers in the online submission form. Responses are followed by a list of relevant readings and resources on interoperability between national, regional, and international data systems.

Q7. What are the key challenges and risks to achieving interoperability at the national, regional, and international levels?

The starting point: Recognizing data interoperability as a techno-political regime

Data interoperability needs to be understood as a layered concept, with a technical and normative dimension. At the technical level, it refers to the "use of common data formats and protocols that enable two or more systems to communicate with one another" ([Bacchus et al, 2024](#)). In the current digital economy, market power is consolidated through the use of restricted Application Programming Interfaces (APIs) for the monopolization of data exchange interfaces. Monopoly power is thus possible when corporations obstruct technical interoperability.

For a fair and competitive digital marketplace, data portability, data accessibility, and data sharing are critical ([Hoffman and Otero 2020](#)). These preconditions are predicated on data format standardization and openness of APIs, in other words, the technical interoperability of data systems.

At the same time, the call for technical standardization to facilitate interoperability should not be equated to mean a call for completely unrestricted data flows between all actors in data markets/innovation ecosystems. The larger question to be answered for data interoperability and development is in relation to the boundaries that governance regimes need to define with respect to the terms and conditions of data access and sharing. The questions for policy are many: How should data flows be directed in various use cases: business-to-business, government-to-business, and government-to-government data? How should data flows be conceived for different markets—national, regional, and international? How should boundaries for data flows be determined in order to achieve a balance between economic and non-economic dimensions of public policy?

These aspects require us to frame the conversation on data interoperability first in its normative dimension. From this perspective, data interoperability refers to the interoperability of data governance regimes—the "set of legal foundations, data handling rules, consumer rights, oversight institutions, and enforcement mechanisms that jointly enable the safe and trustworthy exchange of data flows across jurisdictions" (Bacchus et al., 2024).

Technical interoperability is just one component of an interoperable data governance framework and needs to be calibrated in accordance with the larger normative choices on what data must flow, towards what purposes, to whom, and under what conditions (Gurumurthy and Chami, 2024).

Key challenges and risks to achieving data interoperability at the regional, international levels

Challenge 1. Technical interoperability of data services seen as a sufficient condition for preventing market monopolies

Research suggests that while technical interoperability of data services can reduce duplication and enhance efficiency, this is not enough. In fact, without a robust and nuanced data governance framework—grounded in human rights and public interest norms—technical interoperability can open up privacy vulnerabilities, reinforce monopolies, and entrench existing inequalities. Regulatory oversight is necessary so that dominant players can be kept in check and prevented from creating closed/proprietary technical or operational standards to entrench their market power, thus making it difficult for smaller firms to compete (Russell, 2014, cited in Eaves et al., 2025). Competition law scholars have therefore highlighted the need for regulation to promote vertical interoperability—data exchange that allows services at different levels of the digital value chain to work together, while being more cautious about horizontal interoperability—the ability of products and services at the same level of the digital value chain to "work together" (Bourreau et al., 2022). Without guardrails, horizontal interoperability will entrench the market power of incumbents due to network effects (e.g., Facebook interoperating with smaller social media services). Competition law thus needs a step change in this regard.

Challenge 2. Data interoperability as homogenization of personal data protection standards. This ignores the political, cultural, and economic realities of particular contexts and reinforces digital neo-imperalism

Most discussions of data governance interoperability focus on legal mechanisms for the transfer of personal data with some safeguards. However, anchoring everyone to an acceptable benchmark in consumer rights and privacy protections can drive standards to the lowest common denominator and ignore a whole gamut of data rights. For example, UNCTAD's survey of the data governance frameworks of G20 countries reveals how countries approach the definition of sensitive data very differently. This can be traced to national differences in fundamental beliefs and values about privacy, public interest, and the commercialization of information. Imposing a dominant regulatory grammar of data governance on the majority world amounts to a new form of imperialism that takes away the autonomy of a country to independently determine the overall goal of its digital policy, including the appropriate politico-economic balance it seeks between privacy protection, data security, public innovation, private enterprise, cultural norms around ideas of self and society, etc., in the digital society and economy (excerpted from Gurumurthy and Chami 2024).

Challenge 3. Data interoperability, positioned as unrestricted cross-border data flows, is a decoy in trade agreements, constraining the 'right to regulate' of governments, especially in developing countries

In the guise of furthering equal access to emerging opportunities in digital marketplaces, regional and bilateral free trade agreements often push for unrestricted data flows across borders. This ignores the reality that there is a tension between free cross-border data flows and equitable data innovation. Given the deficits in human and data infrastructural capabilities in developing countries, an interoperable global data governance regime that argues for free flows of data across borders risks heightening the inequalities between data economy leaders and digital latecomers (Leslie et al., 2022). Without the right to access, use, and create value from their data resources for domestic development, developing countries risk being permanently stuck in the low-value segments of the global digital economy as mere providers of raw data and consumers of high-end digital products and services (Digital Economy Report, 2021).

Q9. How can interoperability be advanced in ways that support collaboration while protecting each country's control over its own data, systems, and development priorities?

(i) An interoperable governance regime for training data at the global level

The UN HLAB on AI's proposal for the creation of a global AI data framework that addresses the transversal issues of "availability, interoperability, and use of AI training data" in an integrated manner is critical to unlock the benefits of data innovation for development priorities.

The key elements of the global AI data framework are reproduced below from the UN HLAB's report (from Recommendation 6):

A global AI data framework, developed through a process initiated by a relevant agency such as the United Nations Commission on International Trade Law, and informed by the work of other international organizations, should address the following aspects:

> a. Outlining data-related definitions and principles for global governance of AI training data as distilled from existing best practices, and to promote cultural and linguistic diversity;
>
> b. Establishing common standards around AI training data provenance and use for transparent and rights-based accountability across jurisdictions; and
>
> c. Instituting market-shaping data stewardship and exchange mechanisms at the international level, for enabling flourishing local AI ecosystems—including data trusts and model agreements for facilitating international data access and global interoperability, potentially as techno-legal protocols to the framework.

(ii) The recognition of digital sovereignty and the right to development as a baseline principle in the governance of cross-border data flows

The BRICS Leaders' Statement on the Global Governance of AI underscores digital sovereignty and the right to development as integral to AI governance. Evidently, this vision cannot be realized unless the international governance of cross-border data flows enables the expansion of the "equity of capabilities", which Gurumurthy (2023) has defined as the opportunity for developing countries to make their free choices about the directions of their data economy development without incurring punishing costs/coercion.

The Working Group on Data Governance must recommend that, through the ECOSOC, the annual WSIS review mandate of the CSTD be expanded to include a component on the development of binding principles for 'data flows with rights and equitable development' at the multilateral level.

The tension between sovereignty (the need for all countries to govern their data and algorithmic systems) and internationalism (the need for transnational solidarity and collaboration to regulate digital technologies for the benefit of/prevent harm to people and the planet) in data and AI governance calls for an effective federalist response. A core principle, therefore, is that of subsidiarity (decision-making at the most appropriate governance level) with multi-tiered sovereignty (coordinated action across local, national, and global tiers), in making data governance choices (Ishkhanyan, 2025). Unlike polycentric governance, which emphasizes decentralization, a federalist response retains hierarchical coordination while allowing for adaptive, context-sensitive governance (ibid).

The principles for 'data flows with rights' need an integrated approach to data governance and AI governance, effectively straddling both economic and non-economic dimensions in the governance of cross-border data flows.

The principles must also uphold the policy space of countries to control data flows – for a range of considerations from data protection to preventing foreign actors from surveilling their citizens, ease of data access to support law enforcement, national security (White Paper, 2017) and domestic data industry development (Azmeh and Foster, 2016).

Q11. How can governance and legal frameworks be designed to enable cooperation on interoperability without creating reliance on external actors or systems and remain aligned with public interest?

The road to interoperable data governance must focus on sustainable, inclusive, and democratic futures for all. Data governance frameworks should approach interoperability not as an end in itself but as part of a broader regulatory approach geared towards public value maximization and furthering distributive and democratic integrity in the data economy (benefit-sharing in the data economy and the leveraging of data dividends for public interest and accountability and inclusive citizenship). As a European Parliament Panel study notes, "interoperability without challenging the commodification of data could translate into centralization of data in companies" (Solano et al., 2022).

To ensure that interoperability of data governance creates conditions for promoting the public interest and preserving the autonomy of data communities, the following caveats need to be kept in mind:

(i) If interoperability mechanisms are equated with completely open and unrestricted data access and re-use, there could be adverse ramifications on development sovereignty. Research by Third World Network, for example, demonstrates how the current mode of interoperable data exchange, as unrestricted data access to Digital Sequence Information databases, has heightened the risk of biopiracy in genetic resources (Ramakrishnan, 2024).

Data exchange requires effective oversight mechanisms/licensing conditionalities that prevent data extractivism and enable fair sharing of downstream innovation benefits for society at large (Chandrasekharan, 2025). Embedding "friction-in-design" principles such as purpose limitation, data minimization, and metadata disclosure can slow down extractive data flows and create enforceable pathways for accountability for data misuse. In addition to this, strategic licensing of public and community datasets, with conditions for redistributive outcomes or public value generation, can prevent appropriation and preserve community sovereignty. Evidently, such mechanisms need to be contextualized to consider the specifics of each data ecosystem as they differ in 'actor constellations, technology landscapes, and regulatory constraints' (Hodapp & Henalt, 2022). As discussed above, subsidiarity with multi-tiered sovereignty is important to achieve the right techno-political governance regimes for data that can work for global equity and development justice.

(ii) Interoperability of data governance must be accompanied by safeguards to prevent monopolistic expansion and harmful competition, while harnessing the benefits of data innovation to meet the developmental challenges of communities, incentivizing local and community innovation and diversity of digital services and business models. To prevent technical standardization from entrenching power and market control of dominant players, standard setting for data interoperability must be co-developed through transparent, accountable, and participatory processes, not dictated by industry consortia (Tarkowski et al, 2022).

A literature review and resource list for Track 2: Interoperability

1. Global Digital Compact: Back-sliding to a failed Free-market playbook?, Anita Gurumurthy and Nandini Chami, 2024,
https://botpopuli.net/global-digital-compact-back-sliding-to-a-failed-free-market-playbook/

Relevant extracts:

Blindspot 2. Conflating technical interoperability with the political governance of data

Promoting interoperable data governance approaches is a major objective of the GDC. Interoperability is a term that originated in technical literature to describe the ability of two or more digital systems to work together. Data interoperability, as technical terminology, refers to the use of common data formats and protocols that enable information technology systems to communicate with each other. Maintaining technical interoperability is necessary and useful for datasets and data regimes to be compatible with each other. Yet, extending the minimum

technical interoperability approach to the entirety of data governance is fraught with risks. Data governance, as a systemic framework, may be described as a techno-political regime, incorporating constituent elements of "data handling rules, consumer rights, oversight institutions, and enforcement mechanisms that jointly enable the safe and trustworthy exchange of data flows across jurisdictions." The technical interoperability of data is hence not the same as the complex set of policies comprising the data governance regime aimed at nurturing just and equitable digital ecosystems.

The GDC's exhortation for "innovative, interoperable and inclusive mechanisms to enable data to flow with trust within and between countries to mutual benefit, while respecting relevant data protection and privacy safeguards and applicable legal frameworks" (para 46), is commonly heard in the dominant data governance discourse. The G20 Osaka Declaration also emphasizes the need to advance interoperability of data governance to aid data free flows with trust and harness the potential of data for economic opportunity. Similarly, the UN High-Level Advisory Board on Effective Multilateralism highlights that in the current context of poor interoperability, a system for trusted and secure data flows is urgently needed.

The distinction between data interoperability and data governance interoperability is extremely material to global digital justice. Most discussions of data governance interoperability or data flows with trust focus on legal mechanisms for the transfers of personal data with some safeguards. Anchoring everyone to an acceptable benchmark in consumer rights and privacy protections can drive standards to the lowest common denominator and ignore a whole gamut of data rights. Preserving and promoting data rights in data flows is about addressing the political economy of the platform marketplace – who gains and who loses as data crosses borders in new-age value chains. Every country needs to carefully consider its strategic interests in different sectors and domains that may be best served through cross-border data flows. There is no monolithic roadmap.

As such, global data interoperability in a winner-takes-all market model comes with a huge disadvantage for developing countries. As UNCTAD's Digital Economy Report 2021 (p.131) argues, "While access to data is a necessary condition to benefit from data, it is not sufficient." The economic benefits of data flows are not evenly distributed among countries. In the absence of a globally accepted framework for valuing data resources, developing countries have no recourse for a fair share in the gains of the digital economy. Without the capabilities for data-based innovation, they are in the inevitable position of importing digital products and services – built on the exodus of their own data resources – at exorbitant costs. Data resources, in and of themselves, also do not fetch significant export earnings. The GDC appears to be reconciled to this unequal distribution of data capabilities in shaping the trajectories of future innovation. Para 53's (Rev 4) strategy for international cooperation to build the AI capacities of developing countries is limited to the import and customization of globally developed AI models through the use of locally generated data in their application.

Every country needs to carefully consider its strategic interests in different sectors and domains that may be best served through cross-border data flows. There is no monolithic roadmap.

Data innovation tends to consolidate knowledge monopolies in different sectors. Even where global governance regimes lay down clear rules, such as in the biodiversity domain, interoperability of data can give rise to a new generation of problems that erode the rights of developing countries as well as the public benefits of data innovation (See Box 2).

Box 2. When Interoperability and Open Access Heighten The Risk Of Biopiracy: The Case of DSI Databases

Pushing for interoperability as a foundational norm in data governance in the current status quo risks reinforcing the ills of neoliberal globalization, ignoring the political, cultural, and economic realities of particular contexts. UNCTAD's [survey](#) of the data governance frameworks of G20 countries reveals how countries approach the definition of sensitive data very differently. This can be traced to national differences in fundamental beliefs and values about privacy, public interest, and commercialization of information. Imposing a dominant regulatory grammar of data governance on the majority world amounts to a new form of imperialism that takes away the autonomy of a country to independently determine the overall goal of its digital policy, including the appropriate politico-economic balance it seeks between privacy protection, data security, public innovation, private enterprise, etc., in the digital society and economy. For example, [critics have highlighted](#) how the policy push for mirroring the EU's General Data Protection Regulation (GDPR) standards in domestic data protection regulation in African countries without concern for their "unique social values and economic realities" may jeopardize the emergence of dynamic, home-grown alternatives to development.

The road to interoperable data governance must focus on sustainable, inclusive, and democratic futures for all.

Governance regimes for cross-border data flows need more than technical measures. They need robust legal and institutional mechanisms so that data rights of peoples and nations – encompassing much more than personal data protection – can be upheld through enforceability and redress options. The road to interoperable data governance must focus on sustainable, inclusive, and democratic futures for all.

The GDC should push for an accountable, inclusive, and equitable data governance approach rooted in distributive and democratic integrity. Systematic and inclusive deliberations are needed to move beyond technical interoperability rules in data. A comprehensive global data governance must concern itself with both meta norms for a brave, new data/AI world grounded in digital justice as well as the specific principles, rules, and institutional frameworks reflecting our datafied reality for different international and national policy domains.

2. 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

Relevant extracts:
The Internet Protocol (IP) provides the technical basis for most data flows, and it is supported by thousands of technical standards. Besides technical interoperability, internet data transfers also rely on a layer of commercial interoperability, but the contracts for wholesale internet interconnection have become standardised in practice without the intervention of a global body.

Maintaining technical interoperability and a global internet infrastructure is a prerequisite for digital trade, but it would be difficult to create a minimum common approach or a basic "layer" for data governance in digital trade beyond what is already in place.

The primary focus of "interoperability" within internet policy is to ensure that technical innovations at the firm level are not abused or harm the open internet. In addition to divergent national standards, large internet companies can end up setting different rules and building their own infrastructure, straining the common architecture and governance of the internet. The use of incompatible technical systems is also a risk to competition in the digital sector, if it is used to lock customers in and competitors out.

The flip side of interoperability is the risk of stifling innovation towards higher standards. There is a constant push to make the modern interactive internet faster and more private, which makes it harder for technical systems to remain compatible. We can see this tension in the state-of-the-art technical protocols for privacy in instant messaging software, such as WhatsApp or Signal. The developers have made a very strong case for creating a brand-new technology rather than trying to retrofit privacy to existing internet standards such as email. They argue that this is impossible because of the need for interoperability, although this view is not universal.

Extending the minimum technical interoperability approach to data governance risks anchors everyone to the lowest common denominator that can be agreed between all the parties, dragging down higher standards of consumer and privacy protections. Nuanced discussions of technical interoperability see it as "a foundational element of more complex policies aimed at nurturing healthy and just digital ecosystems".

3. Protocol Power: Matter, IoT interoperability, and a critique of industry self-regulation, Colin Crawford, 2024,
https://policyreview.info/articles/analysis/protocol-power-iot-interoperability

Relevant extracts:

"…processes of technological standardization are inherently political and have long histories: railroads, telegraph networks, shipping containers, internet protocols, and so on. Powerful stakeholders, such as states, corporations, and professional associations each exert their material influence in standard setting in attempts to lock in their preferred (or proprietary) methods and technologies, and thus further extend their power…"

"The setting of an international standard by dominant actors is a particularly productive form of power sharing and market control by determining the "rules of inclusion" and participation on a technical level…Interoperability is thus a key issue which reveals not only the changing shape of tech markets, but also how dominant technological imaginaries influence our ability to understand, negotiate, and ultimately reorganise and govern platform power…"

"While Matter is an open standard which can be accessed and implemented by all developers, the use of the Matter logo as a marketing tool and guarantee of interoperability, as well as access to Alliance networks and resources, requires paying for product certification and/or membership fees, creating a clear hierarchy of influence, power, visibility, and functionality. While the organization rhetorically emphasises its "global" reach and membership, the composition of the Alliance's board of thirty-four members reflects its priority markets, with firms balanced between North America (12), Western Europe (12), and East Asia (10) (CSA, n.d.). Unsurprisingly, market analyses project smart home growth in these highly networked, overdeveloped economies to be much higher than in

South America, Africa, and Central and South Asia, and such priorities shine through (Statista, 2023).

The aspirations of Matter as a universal standard, however, speak to the transnational market capture sought by its creators. At the level of protocol, the Matter standard seeks to dictate the future of the Internet of Things and smart home on the terms of dominant transnational tech firms from North America, Europe, and East Asia by unifying already ubiquitous IP standards. Such a power-sharing arrangement speaks to the vital role of protocol and private standards organizations working closely with industry leaders as ever more objects are made smart, connected, and "ready" not only for one platform but ostensibly for all (Helmond, 2015)."

4. Interoperability in the era of digital innovation: An information systems research agenda, Daniel Hodapp, André Henalt, 2022, https://www.researchgate.net/publication/358413970_Interoperability_in_the_era_of_digital_innovation_An_information_systems_research_agenda

Relevant extracts:

"…advancing interoperability might counteract fragmentation from a technological perspective. This perspective is important in a digital world. However, we still do not know how it interacts with other perspectives focusing on economic, political, or strategic aspects, and what the impact on overall fragmentation can be. Interdisciplinary research is needed to capture the complexity of fragmentation and discern the role of interoperability in this regard."

"Employ a socio-technological perspective on interoperability…literature review shows that there are at least two major conceptual perspectives in past interoperability research…Computer science, and to some extent IS research as well, focuses on a more technological understanding of interoperability by focusing on a specific architectural layer and on the concrete design elements of a particular standard and platform …In contrast, management and business scholars rarely consider these technological features, but aim to understand the institutional dynamics that promote or hinder the diffusion of a particular standard or platform…In the context of digital innovation, a sole focus on either of these two perspectives is unlikely to yield satisfying results. To be specific, considering interoperability in the context of digital innovation without taking the interactions of actors within a particular value space into account is problematic given the distributed nature of digital innovation and the increased heterogeneity of the players…"

"Contextualize the knowledge on mechanisms…Given the diversity of mechanisms to achieve interoperability and their strong intertwinement with the context, it is apparent that the findings behind these mechanisms need to be contextualized to consider the specifics of each ecosystem. Mechanisms that have proven successful for one ecosystem underlying digital innovation might not be appropriate for another ecosystem due to differences in actor constellations, technology landscapes, and regulatory constraints. Therefore, opting for theorizing too early carries the risk that the theoretical insights gained will be too superficial and lack applicability to practice, as some scholars already claim for economic models in the realm of interoperability standard adoption…"

5. The Economics of Shared Digital Infrastructures: A Framework for Assessing Societal Value, David Eaves, Diana Coyle, Beatriz Vasconcellos, Sumedha Deshmukh, 2025, https://www.ucl.ac.uk/bartlett/sites/bartlett/files/2025-04/the_economics_of_shared_digital_infrastructures.pdf

Relevant extracts:

While interoperability reduces duplication and enhances efficiency, poorly managed interoperability can create privacy vulnerabilities,reinforce monopolies or entrench existing inequalities. Without regulatory oversight, dominant players may influence technical or operational standards to entrench their market power, making it difficult for smaller firms to compete (Russell, 2014). Inadequate governance can also create privacy and security risks, particularly in sensitive areas such as health data-sharing. To ensure interoperability delivers broad public benefits rather than concentrating power, governments must establish oversight mechanisms that guarantee fair access, security and competition.

6. Governing data and artificial intelligence for all - Models for sustainable and just data governance, Joan Lopez Solano, Aaron Martin, Siddharth de Souza, and Linnet Taylor, 2022, \https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729533/EPRS_STU(2022)729533_EN.pdf

Relevant extracts:

6.4.4. Interoperability for challenging the dominant data governance model

The interoperability framework could not respond only to the idea of private value creation but as a way to empower communities in vulnerable conditions. The proposals for interoperability in the Data Act promote competitiveness, markets and the freedom to choose for consumers. This definition of interoperability could lead to more sharing and accessing of data but based on the idea of private gain that leads to centralization, exploitation of data and less autonomy for vulnerable communities. Interoperability, without challenging the commodification of data, could translate into the centralization of data in companies, even European ones.235 The interoperability standards do not emerge in empty spaces, but rather in complex power relationships that, if not properly challenged, could translate into the consolidation of the dominant data governance model based on the commodification of data. Interoperability in the EU context thus needs to create conditions for promoting the public interest and the autonomy of communities through the construction of conditionalities for some datasets to flow to the private profit environment and to assure access for public interest institutions like public bodies, media, research institutions and altruistic organizations. The interoperability framework needs to produce the conditions for creating a semi- common perspective,236 cooperative data government and public data trust throughout the Union to rebalance the power relationships that shape the current digital economy.

7. Adversarial interoperability, Cory Doctorow, 2019, https://www.eff.org/deeplinks/2019/10/adversarial-interoperability

8. White Paper of the Committee of Experts on a data protection framework for India, 2017,https://www.lakshmisri.com/Media/Uploads/Documents/White_paper_on_data_protection_in_India.pdf [See page 69]

9. The TPP and the digital trade agenda: Digital industrial policy and Silicon Valley's influence on new trade agreements, Shamel Azmeh and Christopher Foster, 2016, https://www.lse.ac.uk/international-development/Assets/Documents/PDFs/Working-Papers/WP175.pdf [See page 26]

10. A free and fair digital economy - protecting privacy, empowering Indians, Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, 2018, https://www.thehinducentre.com/resources/article24561547.ece/binary/Data_Protection_Committee_Report-comp [See page 87]

11. Alek Tarkowski et al., Generative interoperability: building online public and civic space, Open Future, March 2022, https://openfuture.eu/wp-content/uploads/2022/03/InteroperabilityReport.pdf

Interoperability is then mostly seen as a corrective measure for the deficiencies related to the dominant online platforms and the envisioned impact is 'greater competition among market actors'.

- Improving the market for current platforms will not likely lead to a less centralized ecosystem. Regulation itself will not shift the current power balance away from a few dominant players.

- A market competition approach is not enough. In order to solve the problems we now face in the digital economy, a broader approach should be adopted. We call this approach 'generative interoperability' – a design principle to build a digital space. In the techno-political sphere of digital policymaking, we cannot just address the technical and be deaf to the political.

- Standard setting and governance of standards should be conducted in the open, by dedicated public service entities—with multistakeholder representation. The European digital public space base cannot be established without substantial public investment into both large-scale European-level infrastructures, as well as incubation of smaller initiatives that will populate this ecosystem.

- For the pluralist economy to function, we need to transition to diverse ownership models geared towards local economies, regenerating and sharing wealth rather than extracting it.

- This means investing in public-civic digital infrastructures and varied business models such as the digital cooperative sector.

- Collective action is needed on different levels of government in funding, regulation and procurement. European, national governments, and municipalities all have their roles to play.

12. The Sovereignty-Internationalism Paradox in AI Governance: Digital Federalism and Global Algorithmic Control, Artur Ishkhanyan, 2025, https://link.springer.com/article/10.1007/s44163-025-00374-x

13. Data flows with equity - but, equity of what? Input to Session on Data for Development 2023-24, Intersessional Panel, UNCSTD, Anita Gurumurthy, IT for Change, 2023, https://unctad.org/system/files/non-official-document/cstd2023-24_isp_d_p04_AGurumurthy_en.pdf

14. Data justice in practice: A guide for impacted communities, David Leslie, Michael Katell, Mhairi Aitken, Jatinder Singh, Morgan Briggs, Rosamund Powell, Cami Rincón, Antonella Perini, and Smera Jayadeva, 2022, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4080046 [See page 26]

15. The age of AI nationalism and its effects, Susan Ariel Aaronson, 2024, https://www.cigionline.org/static/documents/Aaronson_306_updated_RtOkp3C.pdf [See page 5]

16. Digital Economy Report, Cross-border data flows and development: For whom the data flow, 2021, https://unctad.org/system/files/official-document/der2021_en.pdf [See page 84]

17. CBD: Proposed solution for digital sequence information promotes inequitable extraction of data, no foreseeable benefit sharing, Nithin Ramakrishnan, 2024, https://twn.my/title2/biotk/2024/btk240801.htm

18. Legal frictions for data openness, Ramya Chandrasekhar, 2025, ://cis.cnrs.fr/en/legal-frictions-for-data-openness-pub/