United Nations University

TECHNOLOGYBRIEF
No. 3, OCTOBER 2023

Regulating Cross-Border Data Flows: Harnessing Safe Data Sharing for Global and Inclusive Artificial Intelligence

Tshilidzi Marwala, United Nations University, Tokyo, Japan
Eleonore Fournier-Tombs, UNU Centre for Policy Research, New York, USA
Serge Stinckwich, UNU Macau, Macau SAR, China

Recommended policy actions

1. Harmonize data protection standards
2. Develop mechanisms to ensure transparency and accountability
3. Promote data localization
4. Develop capacity and infrastructure
5. Promote multi-stakeholder dialogue
6. Implement the principle of mutual recognition
7. Implement the principle of interoperability
8. Promote strong encryption regulations
9. Support research and development initiatives for data protection and privacy challenges, and promote the global dissemination of best practices
10. Facilitate cross-border flow of data essential for the attainment of the SDGs

Introduction

In an increasingly interconnected world, data movement across international borders has become crucial to economic development, innovation and social advancement in an age of interconnected global networks.[1, 2, 3] The international flow of data contributes to economic growth by fostering innovation, enhancing productivity, and facilitating international trade. However, calls to reduce barriers to cross-border data flows have sparked concerns regarding privacy, security, and data protection. The critical policy issue related to cross-border data flows is their potential restriction, particularly through data localization requirements. These requirements force organizations to restrict data access, sharing, and re-use within national borders. However, such restrictions can harm the functioning of markets and the prosperity of societies by limiting the benefits of sharing and re-using data across countries. Nevertheless, it is critical to proportionally address risks, consider the sensitivity of data and understand the purpose and context of processing.

Cross-border data flows are becoming increasingly important in the global artificial intelligence (AI) conversation. The ability to freely and securely transfer data across borders allows AI systems to access diverse information, which is an essential element of debiasing and democratizing AI. However, the emerging patchwork of regulatory approaches to data flows could hinder the deployment of AI systems globally, restrict access to data, and require the duplication of technologies and effort because of data location fragmentation. Therefore, to fully reap the benefits of AI, more interoperable regulatory approaches that enable the free flow of data with trust are needed.[4, 5]

This policy brief discusses the significance of inclusive cross-border data flows. It also proposes an all-encompassing strategy to promote global cooperation to synergize global conversations on cross-border data flows and AI.

What are cross-border data flows?

Cross-border data flows refer to data movement across international boundaries facilitated by digital technologies and communications networks.[6] In the context of AI, such data flows are integral as they enable global access to vast and diverse datasets, essential for training robust and accurate AI models. Furthermore, unrestricted cross-border data transfers support collaborative AI research, enhance the global deployment of AI services, and enable businesses to leverage cloud-based AI solutions. However, these transfers also raise concerns regarding data privacy, security, and sovereignty, necessitating the establishment of international standards and regulations to ensure responsible data sharing and utilization.

Cross-border data flows in China

Before any personal data is transferred out of mainland China, a company must pass a security assessment by the Cyberspace Administration of China (CAC) or obtain a security certification by a third-party certification body designated by the CAC.

On 28 September 2023, China eased the restrictions on cross-border data transfers. The CAC published a draft policy regulating and promoting cross-border data flows.[7] Issues of personal information, security, and the location of data origin are covered in this draft. Experts see this draft policy as a positive sign that China is balancing strong data securitypolicies with promoting data-driven economic growth.

Mainland China and Macau have different regulatory systems for personal data protection and cross-border data flows. At the beginning of 2020, the Macau Special Administrative Region (SAR) Government established the 'Novel Coronavirus Response and Coordination Centre' to comprehensively plan, guide and coordinate the work of all public and private entities in Macau linked to the prevention, control, and treatment of the new viral outbreak. In the context of this policy brief, one of the innovative initiatives that emerged from this centre was launching the cross-jurisdictional blockchain-based health code system to transfer health data.

How the EU's GDPR considers risks in cross-border data flows

The General Data Protection Regulation (GDPR) is a comprehensive data protection law enacted by the European Union (EU) in 2018. It standardizes data privacy laws across all member states and grants individuals greater control over their personal data.[8] Its significance lies in its extensive reach, affecting businesses within the EU and those outside the region that handle EU citizens' data. It is stringent in penalties for non-compliance, thereby setting a global benchmark for data protection standards. The GDPR aims to address several risks associated with cross-border data flows, as shown in Table 1.

Table 1: Main data flow risks addressed by the GDPR

Risk	Description
Data Privacy Breaches	There could be unauthorized access, disclosure, or theft of personal data during transit or at its destination.
Inadequate Data Protection	Data is transferred to countries or territories without robust data protection standards equivalent to those in the EU.
Loss of Data Control	Data subjects lose control over their data when transferred internationally, leading to potential misuse.
Inconsistent Data Protection Standards	Varied data protection laws across countries can lead to inconsistencies in how data is treated and protected.
Data Subject Rights Violation	It is difficult for EU citizens to exercise their rights, such as the right to erasure or data portability, when their data is held outside the EU.
Jurisdictional Conflicts	There are potential conflicts between the GDPR and the data protection laws of the receiving countries.
Lack of Recourse	There are challenges for data subjects in seeking legal recourse in case of data misuse or breach in a foreign jurisdiction.
Surveillance and State Access	There are concerns about foreign governments accessing transferred data for surveillance or other non-commercial purposes without adequate safeguards.
Data Fragmentation	The possibility of data being fragmented and stored in multiple locations makes it challenging to ensure consistent data protection.
Economic Risks	Restrictions on data flows can impact businesses, especially those reliant on global operations and data transfers, potentially hampering economic growth and innovation.

There have been, however, many more initiatives at the national, regional, and international levels to address issues of cross-border data flows. Increasingly, these efforts are becoming linked to regulatory efforts in AI governance. Risks of AI can include data flow risks, especially in relation to AI biases and discrimination, economic exclusion, and harmful uses of AI. Table 2 presents a summary of current regulatory efforts in cross-border data flows as they relate to AI governance.

Table 2: Current regulatory efforts in cross-border data flows

National efforts	
China	China introduced the Data Security Law (DSL) and Personal Information Protection Law (PIPL), which impose strict requirements on data export and set criteria for transferring personal data from China.[9] See new ease of restrictions on page 2: *Cross-border data flows in China*.
Japan	Japan introduced the Data Free Flow With Trust (DFFT) in 2019 to promote the cross-border free flow of data while assuring confidence in privacy, security, and intellectual property rights.[10]
India	The Personal Data Protection Bill (PDPB) is under consideration, emphasizing data localization and restrictions on data transfer outside the country.[11]
Russia	Federal Law No. 242-FZ mandates that the personal data of Russian citizens be stored within the country.[12]
Regional efforts	
European Union	The GDPR sets strict guidelines for data transfer outside the EU, ensuring that data is transferred only to jurisdictions with adequate data protection measures.
Association of Southeast Asian Nations	While there isn't a unified policy, several member states have developed national regulations. The ASEAN Digital Data Governance Framework is a step towards regional harmonization.
Global efforts	
World Trade Organization	While not specific to AI, the WTO discusses e-commerce and digital trade, which can affect cross-border data flows.
Organisation for Economic Co-operation and Development	The OECD provides guidelines on data protection and transborder data flows, emphasizing the importance of interoperability between different data protection frameworks.
Multi-stakeholder initiatives	
Global Partnership on Artificial Intelligence	GPAI is a multi-stakeholder initiative to guide the responsible development and use of AI. While not strictly regulatory, it emphasizes the importance of data governance.
Internet Governance Forum	IGF is a platform where multiple stakeholders, including governments, businesses, and civil society, discuss public policy issues related to the Internet, including data flows.

Areas of divergence in cross-border data flow regulation

National and regional cross-border data flow regulations often differ based on priorities, legal traditions, and sociopolitical contexts. Here are the main areas of divergence:[13]

1. Data localization requirements: Some regulations mandate that certain types of data must be stored and processed within the country of origin (e.g., Russia, India). Others, like the GDPR, allow data transfers under strict conditions, ensuring equivalent data protection.

2. Data transfer mechanisms: Regions like the EU emphasize "adequacy decisions," standard contractual clauses (SCCs), and binding corporate rules (BCRs) for data transfers.[14] Some countries may rely on bilateral agreements or sector-specific arrangements.

3. Scope and jurisdiction: Some regulations have extraterritorial reach (e.g., GDPR affects entities processing EU citizens' data, regardless of location).[15] Others may apply only to entities operating within the country.

4. Data protection standards: The stringency of data protection requirements can vary. The EU's GDPR sets a high standard, while other regions or countries might have less stringent or differently-focused rules.[16] Japan's DFFT emphasizes trust as a fundamental pillar of cross-border data transfer.

5. Government access to data: Concerns about foreign government surveillance can influence data flow regulations. Some countries might restrict data flows to jurisdictions with invasive surveillance practices.[17]

6. Enforcement and penalties: The severity of penalties for non-compliance, as well as the capacity and powers of enforcement agencies, can vary significantly.[18]

7. Individual rights and redress mechanisms: Regulations differ in the rights granted to individuals, such as rights to access, rectification, erasure, or data portability. Mechanisms for individuals to seek redress in case of data breaches or misuse also differ.

8. Exemptions and special provisions: Some regulations may provide exemptions for specific sectors, types of data, or circumstances. For instance, data flows for journalistic, artistic, or research purposes might be treated differently.

9. Cultural and societal values: Cultural attitudes towards privacy, freedom of expression, and government oversight can shape data protection and flow norms. For example, countries emphasizing collective welfare might prioritize cybersecurity or societal stability over individual data rights.

10. Economic and trade considerations: Economic goals, such as fostering digital trade or supporting domestic tech industries, can influence data flow regulations.[19]

These divergences highlight the complexities that businesses and policymakers face in navigating the global digital economy, emphasizing the need for harmonized standards or interoperable frameworks.

Cross-border data flow and sustainable development

Free cross-border data flow is crucial for achieving the Sustainable Development Goals (SDGs) because it enables the sharing of data and knowledge that can be used to resolve global issues such as poverty, hunger, climate change, and inequality.[20] Important data for attaining the SDGs includes information on poverty and discrimination, food safety and nourishment, health and well-being, education, climate and environmental sustainability, and peace and security. It also presents an opportunity to bridge the gaps between the Global North and the Global South. Despite the numerous advantages of free cross-border data flow for the SDGs, some obstacles must be addressed, including privacy, security, and data ownership concerns.[21]

Cross-border data flow and health care

One example of the importance of free cross-border data flow for sustainable development is in health care.[22] By facilitating the interchange of medical information, research data, and expertise across international borders, cross-border data flows are valuable for advancing global health care. The seamless transfer of health-related data facilitates a variety of advantages, and these include:

- Enhanced disease surveillance and response to outbreaks.
- Improved patient care and personalized medicine.
- Promoting global health equity.

Cross-border data flow and climate change

Another example is climate change, which enables scientists, enterprises, and governments to collaborate globally and share information, essential for developing and implementing effective climate action solutions. Examples of how cross-border data flows are being utilized to combat climate change include:[23]

- Transnational data flows are used for global climate modelling.
- Transnational data flows are being used to develop and deploy technologies for renewable energy.
- Transnational data flows are being utilized to enhance disaster response efforts.

Cross-border data flows and new developments in AI

Cross-border data flows are fundamental to the development and application of AI on a global scale.[24] To harness the potential of AI for societal good, a globally harmonized approach to regulating these data flows is essential. First and foremost, nations must have a shared understanding and commitment to prioritize both the ethical use of AI and the protection of individual data rights. A global framework should be built upon transparency, fairness, and accountability principles, ensuring that AI systems are designed and deployed responsibly. By establishing universally accepted standards for data protection and AI ethics, countries can facilitate data exchanges while ensuring that AI technologies safeguard human rights, foster inclusivity, and avoid biases.

Furthermore, such a global regulatory framework should promote open collaboration and knowledge sharing among countries, researchers, and businesses. By encouraging collaborative AI research and development, the international community can address global challenges, from health care and education to climate change and humanitarian aid. This necessitates easing restrictions on data flows for legitimate research and development purposes while maintaining stringent data protection measures. Multi-stakeholder involvement, which includes governments, academia, civil society, and the private sector, is crucial to balance the enablement of AI advancements while ensuring data privacy. International institutions could play a pivotal role in mediating and overseeing the establishment of, and adherence to, a globally harmonized regulatory approach.

Cross-border data flow addresses global disparities and ensures equitable access to opportunities. Thus, it is essential to ensure the Global South is not left behind. Alongside other divides, there is a global divide between data-rich countries and data-poor countries, and this divide has a profound impact on sustainable development at the global level. Cross-border data flow, especially between the Global North and Global South, can enhance the resilience of global common goods by enabling countries with access to valuable insights, technological advancements, and the capacity to make informed decisions.

Cross-border data flows and Internet fragmentation

The increasing emphasis on cross-border data flow regulations has inadvertently contributed to Internet fragmentation.[25] As nations implement varying data protection standards, localization requirements, and access controls, the Internet's once unified and borderless nature begins to fracture into distinct national or regional digital territories. These regulatory disparities can lead to establishing digital barriers, where data, services, and technologies are restricted or segmented by borders. For instance, data localization mandates require companies to store and process data within specific jurisdictions, preventing the free flow of information and potentially creating regional data silos. Such fragmentation of the Internet can stifle innovation, as businesses face increased operational complexities and costs when navigating diverse and sometimes conflicting regulations across countries.

Moreover, this fragmentation impacts more than just the business ecosystem; it has broader societal implications. A compartmentalized Internet can limit access to information, curtail freedom of expression, and reduce the potential for cross-cultural exchanges and global collaboration. Users might find themselves in information bubbles, shaped by regional Internet norms and regulations, leading to a less interconnected global community. Additionally, Internet fragmentation can undermine trust in digital technologies, as users become wary of potential data breaches or misuse in an environment where global standards are lacking. The vision of a globally connected and open Internet, which was foundational to its inception, risks being overshadowed by the rise of digital sovereignties and fragmented cyberterritories.

Cross-border data flows and cybersecurity

While essential for global connectivity and economic growth, cross-border data flows present intricate challenges for global cybersecurity and critical infrastructure protection.[26] The increasing interdependence of digital systems across borders means that vulnerabilities or breaches in one region can have cascading effects on others. For instance, an attack on a power grid in one country can disrupt supply chains globally, given the interconnected nature of modern commerce and infrastructure. As data flows freely across borders, so can cyberthreats, malware, and other malicious tools. The diverse regulatory landscapes and varying cybersecurity standards among nations can create gaps or weak points in global digital defences. Without harmonized cybersecurity protocols, attackers can target these vulnerabilities, compromising local systems and potentially affecting connected systems worldwide.

Moreover, protecting critical infrastructure becomes even more challenging in the face of cross-border data flows. Such infrastructure, which includes power grids, transportation systems, water supply networks, and communication systems, increasingly relies on digital technologies and interconnected networks for efficient operation. As these systems become more interconnected globally, they also become more susceptible to cyberthreats from any part of the world. The challenge lies in ensuring that while data flows remain fluid, digital channels are secure and resistant to potential breaches. Collaborative international efforts are crucial to establishing robust cybersecurity standards and best practices. This involves sharing threat intelligence, coordinating incident responses, and jointly investing in research and development to bolster defences against evolving cyberthreats targeting critical infrastructure.

Another issue that needs to be considered is the asymmetry of capabilities regarding cybersecurity. For example, some countries, especially in the Global North, have more cybercapabilities than others, mainly in the Global South. To deal with the issue of cross-border data flow, we need to, at the least, resolve this cybercapability asymmetry.

Recommendations: a global approach to cross-border data flows

Cross-border data flows are pivotal in promoting global trade and economic growth, especially for businesses in the services sector that heavily depend on international data exchanges. Additionally, these flows spur innovation, allowing businesses, organizations, and governments to tap into worldwide data sets and foster international collaborations. They also enhance global connectivity and understanding by enabling the seamless exchange of information and ideas. However, concerns about data privacy, security, and potential misuse have emerged alongside these advantages, leading to a disjointed global approach to data governance. The present challenge lies in devising a policy that encourages global data flow while addressing these issues.

The recommendations below propose the next steps for fostering a global data-flow framework that will promote safe and ethical AI use, Internet de-fragmentation, and a healthy global cybersecurity ecosystem.

Recommendations for a global cross-border data flow framework

To develop an inclusive strategy for international data flow, policymakers should consider the following strategies:

1. Harmonizing data protection standards: Promote the global harmonization of data protection standards to facilitate data flows without compromising data protection and privacy. This could be accomplished through bilateral and multilateral agreements establishing common data protection standards.

2. Ensuring a secure data flow: Develop mechanisms to ensure data custodians are transparent about their data practices and held accountable for data breaches and mishandling.

3. Promoting data localization: While data localization policies can resolve concerns about security and privacy, an overly restrictive approach can hinder economic growth. The objective of policymakers should be to strike a balance between allowing data flow and resolving security and privacy concerns.

4. Developing capacity and infrastructure: Assist developing nations in constructing the infrastructure and capacity required to participate in the global data economy. This would guarantee a more equitable global distribution of the benefits of data flows.

5. Promoting multi-stakeholder dialogue: Promote a multi-stakeholder dialogue involving governments, the private sector, civil society, and academia to reach a consensus on the norms governing cross-border data flows.

6. Implementing the principle of mutual recognition: Countries can respect one another's regulatory frameworks, recognizing their shared goals, despite differing methods.

7. Implementing the principle of interoperability: Establish cross-jurisdictional standards that enable data transfer in compliance with local laws. Governments can be transparent about their data policies, giving businesses the necessary clarity to operate.

8. Promoting strong encryption regulations: Ensure cybersecurity by strengthening global encryption norms that ensure data security in transit to reduce risks and increase confidence.

9. Conducting research and development: Support research and development initiatives to create innovative solutions to data protection and privacy challenges and promote the global dissemination of best practices.

10. Facilitating cross-border flow of data essential for attaining the SDGs: Nations should share insights, best practices, and lessons learned, leading to collaborative efforts in areas such as poverty alleviation, health care improvement, education, environmental protection, and economic growth. For example, provided that safety, security, ownership and ethics are satisfied, individuals must be able to move their health data across borders to ensure health and well-being.

Conclusion

Inclusive cross-border data flow is pivotal in shaping a globally integrated digital economy that leverages the benefits of data exchange while safeguarding individual and national interests. Constructing a harmonized policy framework that balances economic growth with data protection and security through international collaboration is possible. We can pave the way for a digital future that is inclusive and beneficial for all by promoting transparency, stimulating infrastructure development, and facilitating multi-stakeholder dialogue. Global policymakers should grasp this opportunity to construct a cooperative and inclusive framework for global data governance, propelling society into a new era of prosperity and innovation.

ENDNOTES

[1] https://unu.edu/article/data-lifeblood-global-economy-restrictions-cross-border-data-flows-are-reality

[2] https://www.thecommonwealth-ilibrary.org/index.php/comsec/catalog/book/1118

[3] Marwala, T. (2023). Data in Politics. In: Artificial Intelligence, Game Theory and Mechanism Design in Politics. Palgrave Macmillan, Singapore. https://doi.org/10.1007/978-981-99-5103-1_5

[4] Sekine, T., Legal Framework for Data Free Flow with Trust (DFFT): Trade Agreements as Incubators to Enhance Trust of Data Transaction. In *Changing Orders in International Economic Law Volume 2* (pp. 115-126). Routledge.

[5] Ferencz, J., J. López González and I. Oliván García (2022), "Artificial Intelligence and international trade: Some preliminary implications", *OECD Trade Policy Papers*, No. 260, OECD Publishing, Paris, https://doi.org/10.1787/13212d3e-en.

[6] Chang, Q., Cong, L.W., Wang, L. and Zhang, L., 2023. *Production, Trade, and Cross-Border Data Flows* (No. w31416). National Bureau of Economic Research.

[7] http://www.cac.gov.cn/2023-09/28/c_1697558914242877.htm

[8] Voss, W.G., 2019. Cross-border data flows, the GDPR, and data governance. *Wash. Int'l LJ*, 29, p.485.

[9] Calzada, I., 2022. Citizens' data privacy in China: The state of the art of the Personal Information Protection Law (PIPL). *Smart Cities, 5*(3), pp.1129-1150.

ENDNOTES (Continued)

10 Watanabe, S, 2021. A Study on Schrems II Judgement of the European Court of Justice on International Data Flows - With a Focus on Its Effects on the Data Free Flow with Trust Initiative (Japanese) (No. 21035). https://www.rieti.go.jp/en/publications/summary/21070017.html

11 Maurya, H. and Prasad, S., 2022, October. Data protection laws and a comparative analysis of GDPR and PDPB. In *AIP Conference Proceedings* (Vol. 2519, No. 1). AIP Publishing.

12 Ostrovsky, N.V., 2015. Evolution of the Federal Law" On Production and Consumption Waste". *Management Issues/Voprosy upravleniâ*, (32).

13 Mitchell, A.D. and Mishra, N., 2019. Regulating cross-border data flows in a data-driven world: how WTO Law can contribute. *Journal of International Economic Law*, 22(3), pp.389-416.

14 Kong, L., 2010. Data protection and transborder data flow in the European and global context. *European Journal of International Law*, 21(2), pp.441-456.

15 Chen, S., 2022. Application of US Long-Arm Jurisdiction in Cross-Border Data Flows and China's Response. *US-China L. Rev.*, 19, p.65.

16 López-González, J., Casalini, F. and Nemoto, T., 2021. Mapping approaches to cross-border data flows. *Addressing Impediments to Digital Trade*.

17 Svantesson, D.J.B., 2011. The regulation of cross-border data flows. *International Data Privacy Law*, 1(3), pp.180-198.

18 Daskal, J., 2015. Law enforcement access to data across borders: The evolving security and rights issues. *J. Nat'l Sec. L. & Pol'y*, 8, p.473.

19 Tuthill, L.L., 2016. 14. Cross-border data flows: What role for trade rules?. *Research handbook on trade in services*, p.357.

20 Sergeyeva, A., Abdullina, A., Nazarov, M., Turdimambetov, I., Maxmudov, M. and Yanchuk, S., 2022. Development of Cross-Border Tourism in Accordance with the Principles of Sustainable Development on the Kazakhstan-Uzbekistan Border. *Sustainability, 14*(19), p.12734.

21 Evgenii, S., 2020. Directions of development and regulation of cross-border data flows in international trade. *E-MANAGEMENT*, p.17.

22 Nalin, M., Baroni, I., Faiella, G., Romano, M., Matrisciano, F., Gelenbe, E., Martinez, D.M., Dumortier, J., Natsiavas, P., Votis, K. and Koutkias, V., 2019. The European cross-border health data exchange roadmap: Case study in the Italian setting. *Journal of biomedical informatics, 94*, p.103183.

23 LeSieur, F., 2012. Regulating cross-border data flows and privacy in the networked digital environment and global knowledge economy. *International data privacy law, 2*(2), p.93.

24 Israel, D., 2023. Assessing the Effectiveness of Cross-Border Data Flow Regulations in the Age of Artificial Intelligence (AI). *Available at SSRN 4448648*.

25 Drake, W.J., Vinton, C.G. and Kleinwächter, W., 2016, January. Internet fragmentation: An overview. World Economic Forum.

26 Laidlaw, E., 2021. Privacy and cybersecurity in digital trade: The challenge of cross border data flows. *Available at SSRN 3790936*.

EDITORIAL INFORMATION

About the research
This technology brief is part of a UNU series highlighting specific areas of global technology governance related to the Global South and sustainable development.

Author biographies
Professor Tshilidzi Marwala is the Rector of United Nations University, headquartered in Tokyo, and Under-Secretary-General of the United Nations. He was previously the Vice-Chancellor and Principal of the University of Johannesburg. Marwala has published over 300 papers in peer-reviewed journals and conferences, 27 books on AI and related topics and holds five patents. He is a member of the American Academy of Arts and Sciences, the World Academy of Sciences (TWAS) and the African Academy of Science.

Dr. Eleonore Fournier-Tombs is the Head of Anticipatory Action and Innovation at the UNU Centre for Policy Research, focusing on developing methodological tools and policy recommendations for AI and data at the United Nations. She is also an Adjunct Professor at the University of Ottawa Faculty of Law in Accountable AI and a Global Context and a recurring lecturer on new technologies and cybersecurity for McGill University and Université de Montréal.

Dr. Serge Stinckwich is a computer scientist and the Head of Research at the United Nations University Institute in Macau, a UN think tank taking a human-centred lens to look at how we can amplify the positive contributions of digital technologies for sustainable development and mitigate their risks. His main research interests are in Modelling of Complex Systems, Social Simulation and the impact of Artificial Intelligence on the Sustainable Development Goals (SDGs).

Disclaimer
The views and opinions expressed in this technology brief do not necessarily reflect the official policies or positions of the United Nations University.

Citation
Tshilidzi Marwala, Eleonore Fournier-Tombs, Serge Stinckwich, "*Regulating Cross-Border Data Flows: Harnessing Safe Data Sharing for Global and Inclusive Artificial Intelligence*", UNU Technology Brief 3 (Tokyo: United Nations University, 2023).

ISBN 978-92-808-9149-2