T20 INDONESIA 2022 THINK

Policy Brief

SHARED UNDERSTANDING AND BEYOND: TOWARD A FRAMEWORK FOR DATA PROTECTION AND CROSS-BORDER DATA FLOWS

Task Force 2

Meaningful Digital Connectivity, Cyber Security, Empowerment

Krishna Ravi Srinivas, Research & Information System for Developing Countries (RIS)
Ingrid Schneider, (University of Hamburg)
Wulf Reiners, German Institute of Development and Sustainability (IDOS)

Abstract

Lack of global consensus on data governance is emerging as a major issue in, amongst other things, trade regimes, use of data for development, and regulation of data flows. Convergence or divergence in norms in these areas will determine whether or not any emerging regime complex will be global or fragmented, whether it will enable the potentials of cross-border flow of data to materialize or will suffer from a lack of interoperability. This Policy Brief suggests that the G20 simultaneously underscores the importance of harmonization and strives for consensus on core principles in governing data protection and data flow, and that it also uses competition policy principles to safeguard public interest. While the challenge before the G20 is enormous, it is also an opportunity to provide leadership and shape a global consensus on data governance..

Challenges

At the risk of oversimplification, there are two major approaches in global governance of data: free flow of data and data sovereignty.

Free flow of data is proposed by many countries as a key facilitator in digital transformation, enabling societies to harness data for innovation, growth, economic gains, and valorization of data, and as a paradigm for data management. In fact, cross-border data flows carry a huge potential to generate local economic growth (WEF 2021). Furthermore, with increased interoperability between public services domestically and internationally, including clear cross-border agreements on data ownership, protection, and management of data, data flows bear a great potential for more efficient and transparent government services. At the same time, a compatible, developed (self-controlled) domestic data ecosystem cannot be taken for granted in all countries. Hence, free data flow also increases exposure to dominant (market) actors and the risk of international dependencies.

Data sovereignty, on the other hand, can be understood as the capability of the state to be self-determining regarding its data (including the storage of data, but extending to further aspects of control and power of data, such as information on the existence and possession of data, or its use and re-use) (Hummel et al 2021). In international discussions, it is often presented as an approach that regulates data flows, addressing concerns over privacy, competition, control over the use of data, national security, and prioritizing developmental objectives over commercial interests. In fact, (full) participation in an unrestricted cross-border data transfer system is framed as an increase in vulnerabilities for security and a potential loss of data assets that could otherwise contribute to national development. Data sovereignty often finds expression in a form of techno-nationalism and is typically combined with data localization whereby states incentivize data sharing within the country, regulate it at the regional level, often through bi-lateral and regional trade agreements, and stricter regulations are put on data flows outside the country. The concept thereby also creates boundaries that foster digital exclusion and come with the danger of censorship, or the suppression of free speech.

Among G20 countries, there is no uniformity in terms of principles governing these issues, nor have implicit values and norms guiding their preferences been made explicit. Global data governance is increasingly becoming a patchwork of frameworks (national, regional, bi-lateral and multilateral), and countries do not express a uniform policy on this. Even among various regional trade agreements and bi-lateral agreements there is wide variance in regulating data. The absence of multilateral negotiations on data governance at WTO and the continuation of plurilateral negotiations indicate that a global agreement under the auspices of WTO is still a distant dream. Thus, on account of various factors, complexity in this international arena is increasing, with no progress toward convergence or harmonization. Fragmented regime

constellations and multiple and contradictory frameworks do not augur well for the evolution of data governance for development, international cooperation or for the common good. Hence, the challenge is how to move towards an acceptable solution that reconciles tensions between different perspectives, and between the concepts of “free flow of data” and “data sovereignty”.

Proposals for G20

Three key concepts, which account for controversial elements in the approaches of “free flow of data” and “data sovereignty”, stand out: privacy, size of data spaces and data localization. We propose that finding a common understanding in these areas can result in a framework on data governance that is broadly acceptable. We propose a step-by-step approach on the basis of already established reference works (G20, UNCTAD) and in conjunction with ongoing processes (Global Digital Compact) to structure the debate and identify the space of an “overlapping consensus”. The common understanding can be manifested in diverse outcomes, including guidelines, soft law and typical regulatory frameworks.

Privacy is considered a key value in data governance, but there is no consensus on addressing privacy concerns in regulations. The EU General Data Protection Regulation (GDPR) addresses privacy concerns effectively and has turned into a reference standard for countries around the world, but it may still not be the ideal solution for all, given the costs of regulation and capacity for compliance. In the USA, privacy is a key value, but privacy in data is not regulated by a unified approach or framework such as GDPR. China considers individual privacy and control over data as important and has developed its own model of data governance. However, despite the diverging perspective on data protection and privacy, some shared values and agreed norms may be latent.

The size of data spaces and level of technological advancement are important factors for the global discussion too. Whereas countries with smaller data spaces and/or a lower societal and economic digital competitiveness may see advantages in regulated cross-border regimes for free flow of data to improve development prospects, big data spaces and digitally sovereign actors might be less reliant on strong multilateral frameworks that ensure better access and use of data for everyone.

The localization of data (i.e., the storage and processing of data within a country’s own territory and jurisdiction rather than in servers located abroad) is strongly advocated by some countries, given potential advantages for national security or public interest. China’s legislation on “important data” handled by critical information infrastructure operators (CIIO), Indonesian onshore data centres for public electronic systems operators’ data, or the obligations for critical or sensitive personal data, as proposed by India’s privacy bill, are cases in point. It appears that data localization is mandated for meeting some objectives, in particular when it comes to the sovereignty of the state. The war in Ukraine, and problems in value chains during the Covid-19 pandemic, have fuelled the international discussion on reducing international dependencies. Still, the costs and benefits of data localization and the alternatives have not been fully understood. Some scholars claim that “the perceived benefits, such as growth of the data economy and indirect job creation, accruing from data localization can be achieved through alternative means that are less disruptive for global businesses (Kathuria et.al 2019: 35). At the same time, data localization can facilitate local ICT businesses. Other experts hint at the high energy requirements related to data storage in view of sustainability requirements (Hintemann and Hinterholzer 2020). The powering and setup of the data centre, including the choice of location, therefore comes with consequences for related emissions and the global climate crisis.

The lack of consensus or irreconcilable differences do not need to deter the G20 from taking steps toward developing a balanced framework on data governance. The G20, as a group of major states and economies, not only accounts for the vast majority of data flows, it has also much respectability and legitimacy that should be harnessed for developing a framework that works for developed and developing countries alike. Past work by the T20 and G20 in data governance can be used imaginatively to chalk out a path. The G20 meeting in Osaka in 2019 proposed the concept of "data free flow with trust" (DFFT), and in UNCTAD's 15th session "data flow with trust" (UNCTAD 2021, p. 11) was proposed. The concepts acknowledge the importance of cross-border data flows for, inter alia, the opportunities of the digital economy as well as the role of data for development, in conjunction with national regulations and relevant international commitments. Challenges relating to privacy, security and data protection have been identified in this context, too. These proposals can serve as points of reference and be developed further to build a trust-based framework that promotes cooperation, acknowledging the rights of states to regulate data, although the concept of trust needs further development in this context. A further point of reference should be the UN process to develop a "Global Digital Compact", which aims to improve digital cooperation and features topics of clear relevance for global data governance, including data protection, the avoidance of internet fragmentation, and digital commons as a global public good. Here, the G20 could build on and contribute to the multi-stakeholder digital technology track in preparation for a UN Summit of the Future to advance a common vision for a collective digital future.

In light of the diversity of proposals on global data governance, "[t]he most realistic system of global data governance to both maximize the benefits of data flows and ensure security and privacy is one involving a variety of interoperable regimes" (Goodman and Risberg 2021, p. 2). Hence, the evolution of a balanced, acceptable framework may develop in several steps over time, rather than with one global approach, and build on interoperable national or regional data governance to start building a shared understanding, with the prospect of a stepwise convergence. The process can build on the consensus that data should be governed and harnessed to meet multiple purposes and sustainable development. Further development can borrow from the Rawlsian idea of overlapping consensus to establish a framework in common, and shared understanding (Rawls,1987). While there is no guarantee that this will result in the optimal solution for all functional aspects, this approach can help in moving toward a better understanding of values and principles that underpin regulations. It can facilitate reducing the gaps in understanding and better identification of contentious factors that inhibit development of shared understanding. A common understanding may accept the reality that while harmonization is desirable but not feasible in the short-term, it may help in finding core values that are acceptable to all the parties as well as being optimum, or at least pragmatic, solutions. Moving toward an overlapping consensus may involve nudging and trade-offs, and countries agreeing to work on irreconcilable differences instead of considering them only as constraints. High ambition coalitions of states aiming for deeper integration of data flow regimes may form in this context. However, this group should develop solutions compatible with the overlapping consensus to ensure later convergence on an opt-in basis.

Actionable Policy Recommendations

The G20 should build on the ongoing work on data governance, enhance its engagement with multiple stakeholders and the UN's Global Digital Compact process, identify common values and

positions among members of G20, along with a shortlist of core principles on issues such as privacy, security and data flows, so that a common baseline for policy can be developed. Such a common baseline will enable development of better and shared understanding on global rules and norms and could be fed into relevant multilateral fora, in particular the UN. This may result in an international agreement on core principles, guiding values and best practices on governing data access and control, and on sharing by governments, businesses and other users.

1. Data sovereignty and data localization need to be understood and engaged with; its costs and benefits in view of sustainable development and national security, and how countries incentivize data localization, should be studied in more detail. Any future regime should not centralize, weaponize, or privatize the internet. Crucially, it should strengthen a digital space as a public resource that is global, free, interoperable, climate-neutral and secure as basic preconditions for economic growth, social development and self-expression in an information society. Taking a nuanced approach to data localization, which differentiates between the nature of the data and balances the interests of all stakeholders and cost-effect considerations, can result in a regime that prevents digital exclusion by providing flexibility, combined with stricter compliance on certain data categories.

2. The sheer diversity in data governance regulations and lack of consistency in policy and law on data regulation can be a matter of concern. While this is valid, this need not mean that diversity will result in further fragmentation and divergence with no shared understanding as the most likely outcome. Mapping the diversity is the first step toward identifying an overlapping consensus. The diversity, although perplexing, can be further analysed to find potential scope for convergence and harmonization.

3. When addressing these issues, the G20 should build upon the best practice guidelines or principles related to privacy and cross-border data flows that are found in the literature, in trade agreements, and in the work of the OECD, G20 and APEC Forum. In particular, suggestions from UNCTAD are relevant here, including increased policy dialogue involving all stakeholders (UNCTAD 2021, p. 191).

4. The G20 should provide technical assistance to developing countries to carry out their own assessments of the implications for them of different data governance regimes, taking into account privacy, data market sizes and data localization.

5. “Data free flow with trust” is a good idea. It has been discussed in policy papers and in various statements, but more work is needed on this in terms of theory and practice. In particular, the notion of trust needs further elaboration and contextualization to identify workable models and frameworks. Data flow with trust should inspire and gain confidence of stakeholders, not just states. Hence, the G20 should set up a task force to develop this further in theory and practice.

6. Data free flow, although a good ideal, will not be a convincing one unless it also contributes to development. A key concern on data free flow is that as a principle and practice it could constrain the state’s ability to harness and regulate data for sustainable development. This results in polarizing debates and positions on data for development. The G20 should address this through policy research, and by identifying concerns and objectives of mutual interest, integrating the UN 2030 Agenda for Sustainable Development into the debate as a common

development framework. Through dialogues and stakeholder engagement the concept can be better understood and reflected upon.

7. Although there is some kind of a consensus that privacy is a fundamental value, and that data protection regulation should address privacy concerns, much more is needed in terms of theory and practice. Different data-privacy regimes, with variation in how privacy concerns and protection of privacy are addressed, demonstrate a fragmented approach. Even when countries agree on the importance of privacy, the regimes diverge in terms of the handling of privacy issues. Between the EU's GDPR and a patchwork of regulations that is the norm in many countries, there can be a middle path that is effective as a regulation *and* addresses the core concerns relating to privacy. Convention 108 of the Council of Europe, and 108+ can be deployed as further progress toward harmonization.

8. Fortunately, much progress on addressing privacy issues in data flows is evident in various laws and regulation; this should be taken up further. The G20 can develop a set of core values and guidelines based on this, and best practices that can be adopted. Privacy-enhancing technologies can be promoted and their adoption can be integrated into data governance.

9. Data security and cybersecurity are major issues in data governance. In this, the G20 can also support work to develop guiding principles and best practices. G20 initiatives in capacity development, confidence-building measures and shared understanding on related threats and solutions are possible fields of activity.

10. Understanding the variety of data and the evolving governance milieu on cross-border data flows is essential to identifying and developing frameworks to promote greater interoperability, and/or convergence among domestic regimes so that the goal of data flow with trust can be realized. But it has been found difficult to hold discussions to bridge the different positions on this issue. So, building on themes where there is comfort/common understanding, the G20's commitment to dialogue and decision is necessary for taking the debate forward (OECD 2020, p. 38).

CONCLUSION

The challenges in data governance may appear to be daunting. Nevertheless, it is also an opportunity for the G20 to demonstrate that it can contribute to global policy-making and help in resolving intractable and complex issues. G20 countries have rich experience in addressing data governance issues, although not necessarily on the same principles. G20 countries have also used diverse principles and strategies in regulating cross-border data flows. The implementation of a one-size-fits-all solution is not a realistic immediate development, but reflection on nuanced understandings and practices will help progress towards an "overlapping consensus".

References

M. P. Goodman and P. Risberg, *Governing Data in the Asia-Pacific,* Washington, D.C, Centre for Strategic and International Studies (CSIS), 2021 (CSIS Briefs).

Italian Institute for International Political Studies (ISPI), *T20 Italy - 2021 Final Communiqué,* Rome, ISPI, 2021.

R. Hintemann and S. Hinterholzer, *Rechenzentren in Europa - Chancen für eine nachhaltige Digitalisierung,* Berlin, Borderstep Institut, 2020.

P. Hummel, M. Braun, M. Tretter and P. Dabrock, "Data sovereignty: A Review", in *Big Data & Society*, Vol. 8, No. 1 (January 2021). doi:10.1177/2053951720982012

R. Kathuria, M. Kedia, G. Varma and K Bagchi, *Economic Implications of Cross-Border Data Flows*, New Delhi, Indian Council for Research on International Economic Relations (ICRIER), 2019.

Organisation for Economic Co-operation and Development (OECD), *Mapping Approaches to Data and Data Flows, Report for the G20 Digital Economy Task Force, Saudi Arabia 2020*, Paris, OECD, 2020.

J. Rawls, "The Idea Of An Overlapping Consensus", *Oxford Journal of Legal Studies*, Vol. 7, No. 1 (1987) pp. 1-25.

United Nations Conference on Trade and Development (UNCTAD), *Digital Economy Report 2021*, Geneva, UNCTAD, 2021.

World Economic Forum (WEF), *Advancing Data Flow Governance in the Indo-Pacific: Four Country Analyses and Dialogues*, Cologny, Switzerland, WEF, 2021 (White Paper) https://www3.weforum.org/docs/WEF_Data_Flow_Governance_2021.pdf.

ABOUT THE AUTHORS

First Author and Affiliation	
 Photo	Dr Krishna Ravi Srinivas is a Senior Fellow & Consultant with Research and Information System for Developing Countries (RIS), New Delhi. He does research on, inter alia, issues related to science, technology and innovation related, IP rights, biodiversity and biotechnology and science diplomacy. He has published extensively in these and has been part of many international research projects. He edits Asian Biotechnology and Development Review (ABDR).
Second Author and Affiliation	
	Professor Dr Ingrid Schneider is Professor of Political Science in the Department of Informatics at the University of Hamburg, Germany. Her research fields are technology assessment, governance, law, economy, and ethics of information technology on which she has published numerous publications. Since 1996, she has advised several institutions, including the European Parliament and the European Commission, and has acted as Board Member of various European Scientific Associations and Research Projects. Current research projects are “PRODIGEES - Promoting Research on Digitalisation in Emerging Powers and Europe Towards Sustainable Development” (2020-2025, EU funded) and “Governance of and by Algorithms” (2019-2021).

Third Author and Affiliation	
	Dr. Wulf Reiners is Political Scientist and Head of the Managing Global Governance (MGG) Programme and Senior Researcher at the German Institute of Development and Sustainability (IDOS), Research Programme “Inter- and transnational cooperation”. He is Academic Coordinator of the EU-funded Horizon2020 project "PRODIGEES - Promoting Research on Digitalisation in Emerging Powers and Europe Towards Sustainable Development (2020-2025). His work areas are Global Governance, rising powers, external action and institutions of the EU, and digitalisation.