WE NEED TO TALK ABOUT **DATA**

FRAMING THE DEBATE AROUND FREE FLOW OF DATA AND DATA SOVEREIGNTY

INTERNET & JURISDICTION
POLICY NETWORK

The Internet & Jurisdiction Policy Network is the multistakeholder organization fostering legal interoperability in cyberspace. Its stakeholders work together to preserve the cross-border nature of the internet, protect human rights, fight abuses, and enable the global digital economy. Since 2012, the Internet & Jurisdiction Policy Network has engaged more than 400 key entities from six stakeholder groups around the world including: governments, the world's largest internet companies, the technical community, civil society groups, leading universities and international organizations.

For more information, visit www.internetjurisdiction.net

Supported by:

Federal Ministry
for Economic Affairs
and Energy

on the basis of a decision
by the German Bundestag

Report Citation:
De La Chapelle, B. and L. Porciuncula (2021). We Need to Talk About Data: Framing the Debate Around Free Flow of Data and Data Sovereignty. Internet and Jurisdiction Policy Network.

INTRODUCTION

Words matter in policy debates. Even when facing profound digital transformations, reliance on existing concepts to guide policy has a natural pull. Yet, expressions with a strong historic baggage can trigger both enthusiastic support or fierce opposition, irrespective of their actual relevance to the issue at stake. A topical illustration is our collective difficulty to deal with the challenges raised by the massive amounts of data that now underpin almost all human activities across geographies.

On the one hand, "Free Flow of Data" is advocated by many as a critical enabler of digital transformation, innovation, economic growth and social benefits. At the same time, various concerns related to privacy, taxation, competition, security, and even the democratic process, have prompted policy initiatives invoking the notion of "Data Sovereignty".

"Free flow" and "sovereignty" are terms which strongly resonate with policy-makers, businesses and even citizens. Their coupling with the word data too often generates visceral reactions and intense exchanges devoid of nuance, in a context of heated debates about the impacts of digitalization and growing geopolitical tensions. The diversity of sectoral silos where discussions are conducted worsens the situation and makes solutions even harder to find.

This framing report seeks to unpack these two polarizing expressions to better understand actors' perspectives, and shift the debate towards reconciling apparently conflicting approaches. The goal is not to provide a comprehensive overview of all the issues and stakeholder views, but to offer a holistic snapshot of the concerns and prominent perspectives to kick-start further debate.

The report is organized in three self-explanatory parts: Data, Free Flows of Data, and Data Sovereignty. It concludes, in Moving Forward, with a call to reframe the discussion, harness emerging innovative approaches, and engage in a much needed global, multistakeholder and cross-sectoral debate.

This report aims to raise the awareness of the general audience and serve as a resource to policy shapers and practitioners in the public and private sectors to help frame the debate around data. The Secretariat of the Internet & Jurisdiction Policy Network (I&JPN) made a deliberate effort to capture diverse views and perspectives, and will organize, on the basis of this initial framing, further consultations across sectors and regions to expand the understanding of these evolving concepts and their policy implications.

Building the methodology for addressing the problems of the digital age is as important as addressing the problems themselves. Developing a common framing of issues is a prerequisite. We hope this report will help catalyze a more nuanced and collaborative discussion. How we collectively address the challenges and opportunities pertaining to the governance of the Datasphere will determine the society we will build and live in.

ACKNOWLEDGEMENTS

When preparing this report, the I&JPN Secretariat held consultations with various stakeholders in the form of virtual roundtables and individual interviews with policy-makers, experts and practitioners. A survey to the I&JPN community was also launched, which received over one hundred contributions. The list below reflects some of the policy actors who engaged in individual meetings and roundtables with the I&JPN Secretariat. The report has however been drafted under the sole responsibility of the I&JPN Secretariat and does not engage the actors listed. The I&JPN Secretariat is grateful to **the German BMWi for its support** and **thankful to** all those who shared their expertise and experience which helped the production of the report:

Susan Aaronson, Research Professor and Director, Digital Trade and Data Governance Hub, George Washington University and Senior Fellow, Economics, CIGI • **Carlos Affonso Souza**, Director, ITS Rio • **Fiona Alexander**, Research Professor and Director, Digital Trade and Data Governance Hub, George Washington University and Senior Fellow, Economics • **Brigitte Benoit Landale**, Deputy Head, Switzerland - International Law Section at Federal Department of Foreign Affairs (DFA) • **Oli Bird**, Head of International Policy, United Kingdom - Office of Communications (Ofcom) • **Christian Borggreen**, Director of International Policy, Computer & Communications Industry Association • **Jorge Cancio**, Deputy Head of International Affairs, Switzerland - Federal Office of Communications (OFCOM) • **Vint Cerf**, Chief Internet Evangelist, Google • **Mario Cimoli**, Deputy Executive Secretary, UN Economic Commission for Latin America and the Caribbean • **Marina Comninos**, Co-CEO & COO, essDOCS • **Fernanda Domingos**, Federal Prosecutor, Federal Prosecutors Office of São Paulo, Brazil • **Roger Dubach**, Deputy Director, Directorate of International Law Switzerland (DFA) • **Raul Echeberria**, Executive Director, ALAI - Latin American Internet Association • **Andrin Eichin**, Policy Advisor, Switzerland - Federal Office of Communications (OFCOM) • **Anne Joséphine Flanagan**, Data Policy & Governance Lead, World Economic Forum • **Lise Fuhr**, Director General, European Telecommunications Network Operators' Association • **Carl Gahnberg**, Senior Policy Advisor, Internet Society • **Urs Gasser**, Executive Director, Berkman Klein Center, Harvard • **Jan Gerlach**, Public Policy Manager, Wikimedia • **Carlos Grau Tanner**, Director-General, Global Express Association • **Robyn Greene**, Privacy Policy Manager, Facebook • **Rudolf Gridl**, Head of Unit, Internet Governance, Germany - Federal Ministry for Economic Affairs and Energy (BMWi) • **Ilham Habibie**, President Director, PT. ILTHABI Rekatama • **Hiroki Habuka**, Deputy Director of the Digital Economy Division, Japan - Ministry of Economy, Trade and Industry • **Clara Iglesias Keller**, Visiting Researcher, Humboldt Institute for Internet and Society • **Peter Kimpian**, Director of Information Society and Action against Crime, Council of Europe • **Michael Kende**, Professor, Graduate Institute for International Studies and Development • **Hariramchakraborthy Janakiraman**, Head – Global TSC Products and TSC Solutions, Int'l Australia and New Zealand Banking Group Ltd • **Tomas Lamanauskas,** Managing Partner, Envision Associates • **Klaus Landefeld**, Vice Chairman of the Management Board, Director Infrastructure & Network, ECO • **Javier López González**, Senior Economist, OECD • **Riccardo Masucci**, Global Director of Privacy Policy, Intel • Corynne McSherry, Legal Director, EFF • **Angel Melguizo**, Vice President, External & Regulatory Affairs, Latin America AT&T DIRECTTV • **Lim May-Ann**, Managing Director, TRPC, Executive Director, Asia Cloud Computing Association • **Mia Mikic**, Director at Trade, Investment and Innovation Division, UNESCAP • **Kenta Mochizuki**, Deputy Counselor for International Affairs, Personal Information Protection Commission of Japan • **Greg Nojeim**, Senior Counsel and Director, Freedom, Security and Technology Project, Center for Democracy & Technology (CDT) • **Michael Nelson**, Director of Technology and International Affairs Program, Carnegie • **Carolyn Nguyen**, Director, Technology Policy, Microsoft • **Georgina Nunez**, Economic Affairs Officer, UN Economic Commission for Latin America and the Caribbean • **Sissi de la Peña**, Regional Digital Commerce Manager, ALAI - Latin American Internet Association • **Christian Reimsbach**, Economist, Digital Economy Policy Division, OECD • **Sasha Rubel**, Programme Specialist, Digital Innovation and Transformation, UNESCO • **Michael Rose**, Data Policy, Google • **Fernando Rojas**, Division of Production, Productivity and Management, UN Economic Commission for Latin America and the Caribbean • **Ashwin Sasongko Sastrosubroto**, Member, Indonesian National ICT Council • **Nicolas Schubert**, Head of Department, Digital Economy, Chile - Ministry of Foreign Affairs • **Thomas Schneider**, Ambassador and Director of International Affairs, Switzerland - Federal Office of Communications (OFCOM) • **Mark Surman**, Executive Director, Mozilla Foundation • **Alissa Starzak**, Head of Public Policy, Cloudflare • **Dan Svantesson**, Professor, Bond University • **Jeni Tennison**, Vice President and Chief Strategy Adviser • **Lee Tuthill**, Counsellor, Trade in Services, World Trade Organization • **Yvo Volman**, Head of Unit, Data Strategy, European Commission • **Andrew Warnes**, Assistant Secretary, National Security Branch, Australia - Department of Home Affairs • **John Wilbanks**, Chief Commons Officer, Sage Bionetics • **Mathieu Weill**, Head of Digital Economy Department, France - Ministry of Economy • **Richard Whitt**, President, GLIA Foundation • **Miriam Wimmer**, Director of the Brazilian Data Protection Authority (ANPD) • **Moctar Yedaly**, Head, Information Society Division, African Union Commission • **Robert Young**, Legal Counsel, Canada - Department of Global Affairs

The non-attributed quotes in this report are all taken from discussions with the consulted stakeholders through virtual roundtables and interviews.

The Report was authored by the Secretariat of the Internet & Jurisdiction Policy Network: **Bertrand de La Chapelle**, Executive Director and **Lorrayne Porciuncula**, Director of the Data & Jurisdiction Program. The development of this Report was supported by **Paul Fehlinger**, Deputy Executive Director, **Ajith Francis**, Policy Programs Manager, **Sophie Tomlinson**, Communications & Outreach Manager and **Juri Wiedemann**, I&JPN Young Professional.

Design and Layout: **João Pascoal Studio** www.joaopascoal.com | Illustrations: **Leremy Gan** www.leremy.com

EXECUTIVE SUMMARY

1. ON DATA

Beware of analogies. Analogies are useful to approach unfamiliar situations, but taking them too literally can lead to misguided policy choices.

Data is multidimensional. The world of data is growing and diverse, prone to overlapping modes of classification and formed by numerous actors connected by complex relations and value chains.

Data has unusual properties. Data is different from goods and services, as a non-rivalrous resource which can be replicated and combined in numerous value chains without being depleted.

Location of storage and processing is not all that matters. Who collects, processes or accesses data - and for what purpose(s) - is of high relevance.

2. ON FREE FLOW OF DATA

The shadow of the free trade debate. Discussions around Free Flow of Data are strongly influenced by existing tensions around free trade.

Free Flow of Data is a topic high on global policy agendas. Cross-border data flows are a direct result of the internet architecture, but remain difficult to address in existing multilateral fora.

Concerns exist regarding digital interdependence dynamics. Cross-border data flows raise various concerns, overlapping security, economic and human rights dimensions.

Cross-border data flows depend upon trust. Dealing with potential misuses of data while preserving its free technical transit requires dedicated trust-building frameworks.

3. ON DATA SOVEREIGNTY

Digital challenges to territorially-based sovereignty. The non-geographic architecture of the internet is challenging the Westphalian paradigm underpinning our current international system.

Data Sovereignty is peddled as a panacea to many concerns. The multifaceted notion of Data Sovereignty is both explained and perceived in very different, sometimes conflicting, ways.

Implementation pitfalls. Data Sovereignty measures come in different guises, and their implementation is prone to unintended consequences, with systemic effects if generalized.

Dealing with multiple jurisdictions. Data connects with territories and jurisdictions in multiple ways, producing an ecosystem of overlapping applicable rules and redefining the exercise of sovereignties.

4. MOVING FORWARD

Addressing the challenges related to the governance of the growing Datasphere requires:

Organizing a global multistakeholder debate across sectors.

Reframing the discussion towards more nuance and common objectives.

Exploring and fostering innovative approaches in tools, frameworks and concepts.

THE REPORT AT A GLANCE

1 ON DATA

8 Beware of analogies

11 Data is multidimensional

14 Data has unusual properties

17 Location of storage and processing is not all that matters

2 ON FREE FLOW OF DATA

21 The shadow of the free trade debate

24 Free Flow of Data is high on global policy agendas

28 Concerns exist regarding digital interdependence dynamics

31 Cross-border data flows depend upon trust

3 ON DATA SOVEREIGNTY

35 Digital challenges to territorially-based sovereignty

38 Data Sovereignty is peddled as a panacea to many concerns

41 Implementation pitfalls

45 Dealing with multiple jurisdictions

4 MOVING FORWARD

50 Organizing a global multistakeholder debate across sectors

51 Reframing the discussion towards more nuance and common objectives

52 Exploring and fostering innovative approaches in tools, frameworks and concepts

CHAPTER

1

ON DATA

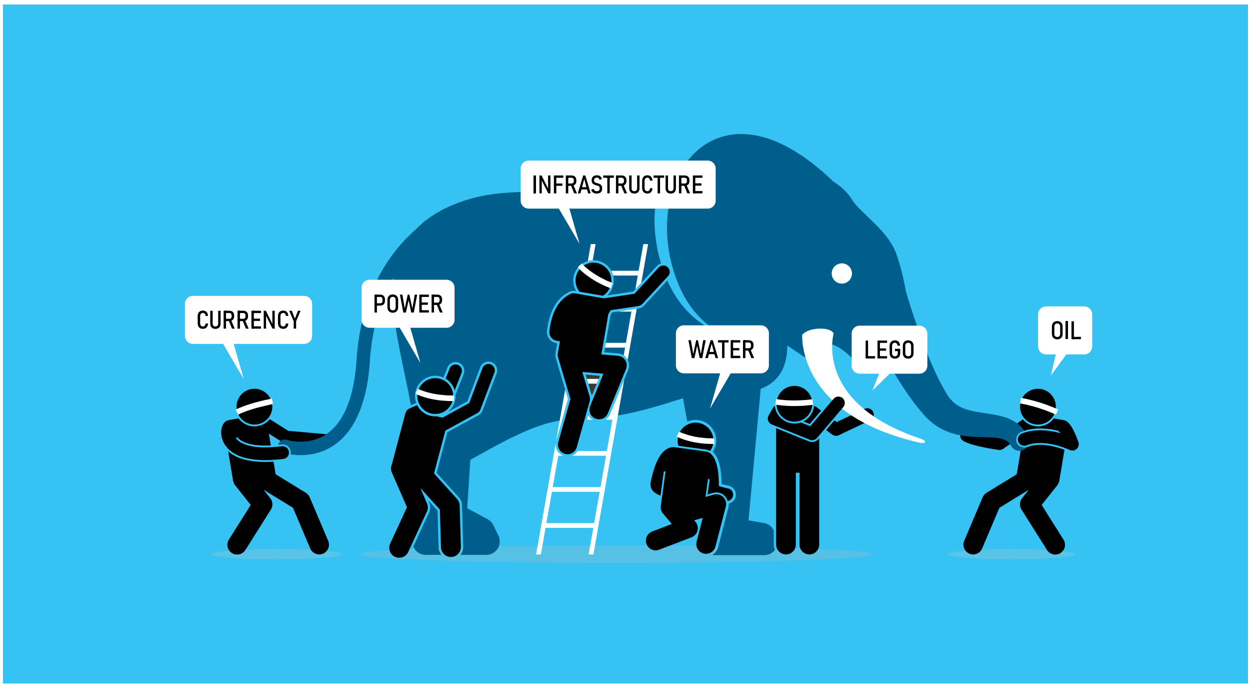
Data is just data. It is not "like" anything at all. Data should be regulated carefully, with consideration for what it does in various situations for different types of firms and for consumers. Trying to shove "data" into existing mental models is likely to do more harm than good. It makes it easier to ignore the unintended consequences of various types of regulations.

DEBORAH ELMS

Executive Director, Asian Trade Centre

- *Beware of analogies*
- *Data is multidimensional*
- *Data has unusual properties*
- *Location of storage and processing is not all that matters*

BEWARE OF **ANALOGIES**



Analogies are useful to approach unfamiliar situations, but taking them too literally can lead to misguided policy choices.

A profusion of analogies aims to bring us back to the familiar

Whenever new phenomena emerge, analogies help people make sense of them. The growing importance of data is no exception. In that regard, the most popular analogy is "data is the new oil", attributed to Clive Humby, mathematician and architect of the Tesco Clubcard, who coined it in 2006. The powerful image has since been promoted by numerous politicians and business people and in 2017 the Economist qualified data as "the most valuable resource" with a cover representing the largest digital companies as petroleum drilling platforms.

Since then, and in large part in reaction, numerous expressions starting with "Data is the new…" have proliferated, insisting that data should be compared instead to: currency, air, water, gold, nuclear power, capital, power, labour, infrastructure[1], blood, king, natural resource, fuel, Lego, and many other analogies, including the provocative "data is the new avocado".[2]

[1] Bayat, A. and P. Kawalek (2017), *Data as Infrastructure*, National Infrastructure Commission, https://abdn.pure.elsevier.com/en/publications/data-as-infrastructure.

[2] Asian Trade Centre (2019), "Data is the new avocado", *Talk it Trade*, http://asiantradecentre.org/talkitrade//data-is-the-new-avocado.

Each analogy may provide useful insights

The “data is the new oil” meme replicated virally because, indeed, as oil powered the last industrial revolution, data is enabling the current one. Expressions like data mining or refining data (in order to extract value or create elaborate knowledge) also contributed to reinforce the analogy.

Likewise, however far-fetched, each analogy highlights important aspects of data. Like water, data flows irrigating our societies and economies are essential for their flourishing. Like currency, access to data can be a counterpart for other goods, as the business model of social media or the recent deal between Israel and a COVID-19 vaccine provider demonstrate.[3] Data can clearly be leveraged as an instrument of power and its progressive accumulation is a major capital asset for a corporation. The Lego analogy was meant to highlight the need for vast amounts of diversified data to feed Artificial Intelligence (AI) and machine learning (ML) to avoid errors or biases.[4] And the avocado comparison points to data sometimes having a limited “shelf-life” depending upon its intended use.

Only the diversity of perspectives provides a complete picture

Like in the proverbial story of the blind men and the elephant, each category of actor or provider of a particular analogy usually focuses on one dimension of data, looking at it from their specific – albeit necessarily limited – vantage point. The proliferation of alternative comparisons is therefore useful in providing a fuller picture and demonstrating the very complex and multi-dimensional nature of data.

More importantly, no single analogy is entirely accurate, nor should it be taken literally to the full extent. In particular, many of the new comparisons aim at showing the limits of the dominant oil analogy. In particular, unlike oil, data is not extracted from nature but rather a human (or machine) produced resource, and it is neither finite nor naturally located in a particular geographic region.

Incautious reliance on analogies can lead to misguided policy choices

Analogies are different from metaphors. Metaphors are mostly rhetorical or poetic (e.g. Shakespeare’s “All the world’s a stage”), but analogies are often used to make a point regarding the original term. Connections with other notions may then imply desirable actions. Choosing the wrong analogy (or too extensive an interpretation of a valid one) as a basis for policy can, at the very least, be distracting, and ultimately actually lead to unsound regulations, laws and governance models.

In that regard, “Data is the new oil” brings to mind historic attitudes and policies hardly appropriate to data: the desire to hoard it locally as scarce resource and a strategic asset, a Malthusian incentive to use it sparingly, apply a consumption tax to pay for the infrastructure or restrict its circulation, and most importantly, a reference to the breaking up of oil-refining monopolies (e.g. Standard Oil) as inspiration for the regulation of dominant tech giants. Analogies must be used with caution when dealing with new phenomena.

[3] Estrin, D. (2021), “Vaccines For Data: Israel’s Pfizer Deal Drives Quick Rollout — And Privacy Worries”, NPR, www.npr.org/2021/01/31/960819083/vaccines-for-data-israels-pfizer-deal-drives-quick-rollout-and-privacy-worries.

[4] Woodward, M. (2018), “Data is the New Lego”, *True Fit*, https://www.truefit.com/en/Blog/August-2018/Data-is-the-New-Lego.

Quotes from consulted stakeholders

I don't really like this idea that data is the new oil or the new gold. Gold and oil are limited, there's only a certain amount of that on the planet. Data gets created constantly from other data, over and over again. So it's limitless.

Data is not a stash of cash you can put safely under your pillow and then get value from it.

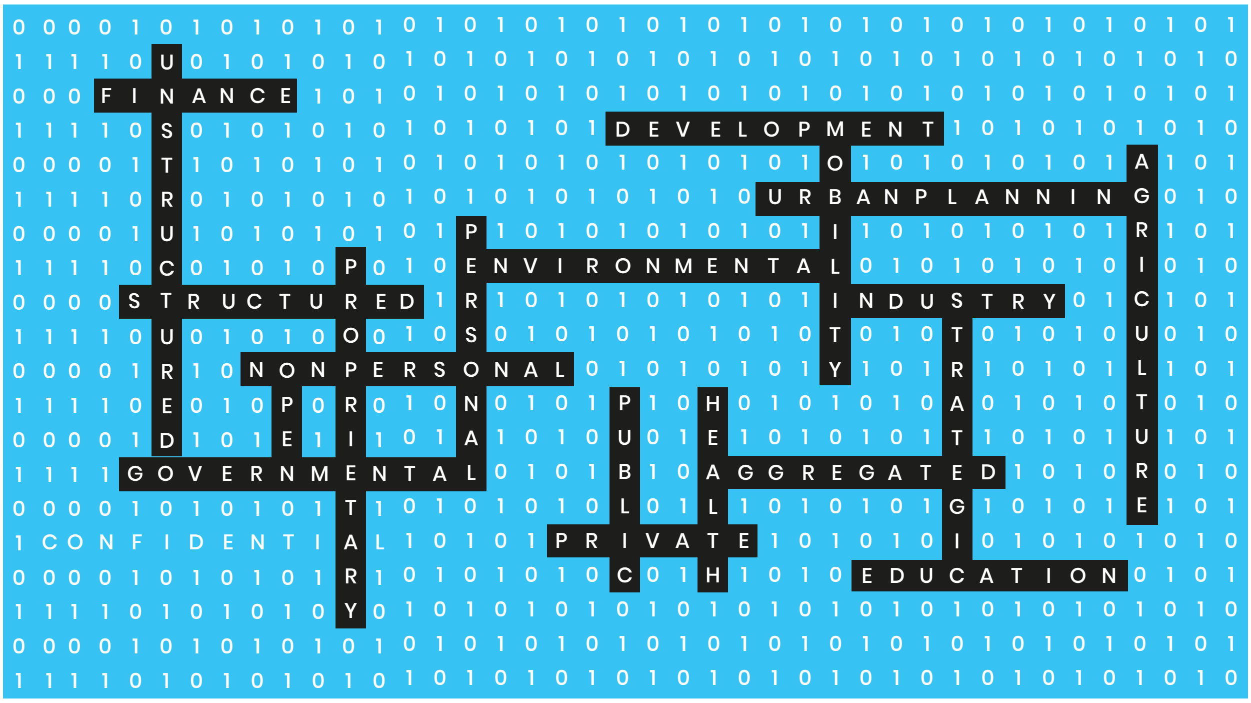
There is a laziness with metaphors: it communicates that you don't need to go into details because this one thing that seems new, actually you already know how it works and what are the impacts.

We should think more in terms of examples of data flows, which are precise, rather than in analogies, which can be insightful, but incomplete.

Either don't use an analogy, because there's not one good one, or use multiple ones, depending on the angle.

Whatever metaphor we use, data is always different in some way, which is why there are risks with using metaphors.

DATA IS **MULTIDIMENSIONAL**



The world of data is growing and diverse, prone to overlapping modes of classification and formed by numerous actors connected by complex relations and value chains.

The exponential growth and diversification of data

The volume of data produced by modern economies and societies is hard to grasp in a tangible way. General users may be familiar with gigabytes (GB) or maybe terabytes (1 000 GB). Yet, industry deals with data volumes expressed in peta-, exa-, or zettabytes (1 ZB = 1 billion TB) and even yottabytes (1 YB = 1 000 ZB). If a byte were a grain of rice, it is estimated that one zettabyte would cover the entire Pacific Ocean in rice.

By 2025, the volume of data produced is expected to hit worldwide 175 ZB, growing at an exponential rate of 60% CAGR.[6] More than 80% of this volume will be unstructured data and Internet of Things (IoT) data is expected to represent close to half of the overall amount. More importantly, a growing portion of the data produced would be treated on the edge (e.g. inside autonomous vehicles, devices or factories) and in real-time instead of stored and processed in large data centers as is the case today. At the same time, storage of data by companies themselves in their own enterprise servers is strongly migrating to public cloud services.

[6] Reinsel, D., J. Gantz and J. Rydning (2018), “Data Age 2025: The Digitalization of the World, From Edge to Core”, *IDC White Paper*, https://itupdate.com.au/page/data-age-2025-the-evolution-of-data-to-life-critical-.

There are multiple ways to classify data

Data is not a monolith. Numerous studies undertaking classification of data only confirm the multiplicity of ways this can be done. The most common distinction, particularly in regulations, is between personal and non-personal data. Yet, many other dichotomies can also be considered, including, but not limited to: public vs private, confidential or not, structured vs unstructured, open vs proprietary, geo-tagged or not, anonymized vs pseudonymized, stored vs real-time, or human generated vs machine produced data.

Classifications can also reflect or be driven by: the nature of the data (e.g. numerical, textual, pictorial), the degree of refinement (e.g. raw, aggregated, information, knowledge), the intended use (e.g. research, marketing, compliance, AI), the imposed access conditions or legal protections, and most importantly, the very diverse economic sectors it originates from or is being employed in (e.g. health, finance, commerce, industry, transportation, urban planning).

Classification boundaries are blurred and overlapping

While there is general agreement that different regulations could legitimately apply to different types of data, the multi-dimensional nature of classifications is a serious obstacle to universal taxonomies and simple-to-implement rules.

Even the fundamental distinction between personal and non-personal data can be blurry, as some anonymized data can be processed or recombined to reveal meaningful patterns of individual behavior. Personally Identifiable Information (PII) is a more focused notion to cover data that allows to distinguish one person from another. Furthermore, data collected in a particular sectoral context can be meaningful and useful in several others.

In parallel, data collected by public authorities (e.g. air quality, climate, satellite imagery) can be made available through open data schemes or licenses to allow the development of commercial applications (e.g. weather insurance based on meteorological data). Likewise, business-generated data can powerfully inform public policies and their implementation (e.g. geo-tagged traffic data from vehicles used in urban planning).

The importance of data value chains

The tsunami of raw data needs quantitative and qualitative processing to turn into something usable, which creates more data and metadata. Every actor, for its own use or for the benefit of others, therefore aggregates, filters, analyzes, extracts patterns, feeds its own data into artificial intelligence or executes various transformations and combinations with third party data along value-generating steps.

In addition, complex external value chains involve numerous intermediary actors with increasingly diversified and innovative roles, as the data economy develops. Ensuring the integrity of data and its protections along the chains of transmission therefore becomes increasingly challenging, and vastly depends upon the modalities of data access (e.g. difference between bulk transmission or access through APIs). In addition, the value of data varies according to the potential user: what is priceless for one may be meaningless for others, and timeliness might also be a factor.

The created value can be economic, societal, or most often both. Public policies and corporate decisions impact the balancing of the two as well as the distribution of value among different stakeholders. Unfortunately, societal and economic value of data is extremely hard to measure and thus not satisfactorily reflected in accounting practices, nor GDP measurement.[7]

[7] Ker, D. and E. Mazzini (2020), "Perspectives on the value of data and data flows", OECD *Digital Economy Papers*, No. 299, OECD Publishing, Paris, https://doi.org/10.1787/a2216bc1-en.

Quotes from consulted stakeholders

Some kind of common agreement is going to be needed across international borders, other than simply looking at every bit that flows and making decisions bit by bit, which is simply not possible.

Top-down classifications are always tricky. You lock yourself in. We need more flexible and bottom-up approaches to collectively build different models of classification.

The elephant in the room is personal data. The decision is pretty binary and, for some, too simplistic to divide data into personal and non personal data. But that is for a very good reason, which lies in the history of the European continent, of universal human rights, of promoting the idea that personal data should be protected and that all individuals are entitled to decide on their data. And that all countries and stakeholders have a positive obligation to uphold this right.

The most important element that we're seeing in these questions is the fuzziness in the distinction between personal and non personal data.

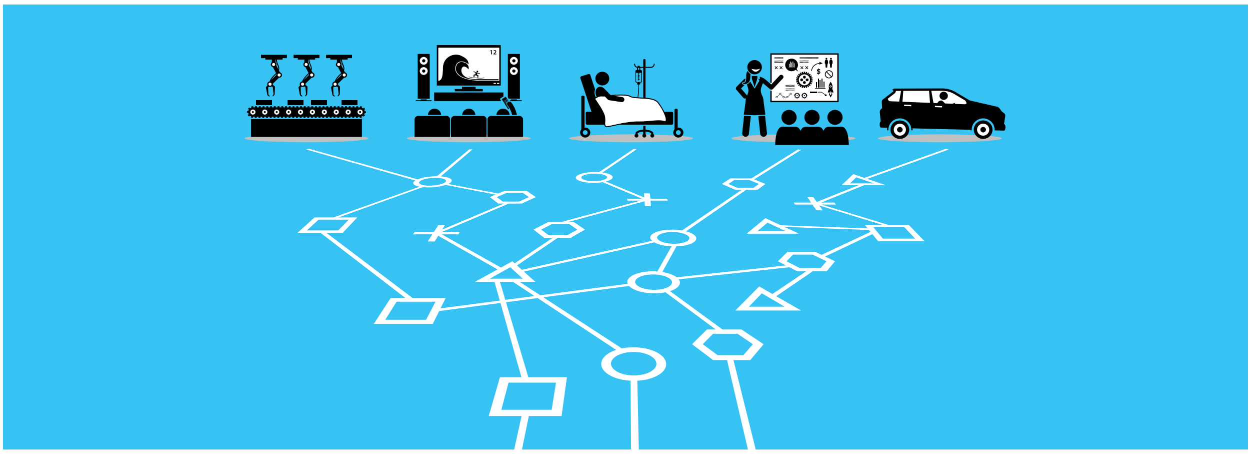
GDPR is clearly one of the sticking points. People seem to have different views on what's personal data and what's non personal data , so until we can kind of get some commonality around that I don't know how we will get to a framework.

Pretty much all data about a person and their environment becomes health data. Where my phone is and what I am buying to eat is now health data, as well as geolocation data and bank data.

Environmental data looks like environmental data until I need to know if that is the air pollution that is driving asthma in my kid. And so it is tough because when any data touches health data it suddenly acquires protections of health data. It is the query and the joining that make data jump across sectors in a way that is hard for regulations to follow.

The differentiation between personal and non-personal data is more akin to a spectrum. There is some data which can easily be put in specific buckets, and others which can't.

DATA HAS UNUSUAL PROPERTIES



Data is different from goods and services, as a non-rivalrous resource which can be replicated and combined in numerous value chains without being depleted.

A non-finite, durable and non-rivalrous yet excludable resource

In many regards, data is very different from classic goods and services. First of all, data is far from a limited resource, as its exponentially growing volume attests. Moreover, data is generative: data begets more data through analysis. Data is also durable, meaning it can be used without being depleted. It is therefore much more than a renewable resource (i.e. one that has the capacity to replenish faster than the rate of average consumption).

More importantly, data is non-rivalrous. A good is rivalrous if its consumption or use by someone prevents others from simultaneously doing the same, or if it reduces the available supply for others. Most tangible goods are rivalrous, including fuels such as oil or minerals like gold. Contrastingly, several people or entities can simultaneously use the same data and use by one actor does not reduce the ulterior capacity of others. Data can even be considered "anti-rivalrous", a term coined by Steven Weber in relation to open source software, to describe goods where the more people use them, the more utility each person receives.[8] A topical example for data is: the more users share their (anonymized) location in traffic, the more accurate congestion maps become for everyone, even for those not contributing.

Unlike physical goods, data can be easily replicable, shareable, transmissible, and remotely accessible or controllable. This in addition is achieved at increasingly minimal cost, thanks to the plummeting price of storage capacity, processing power and communication services.

Data is nonetheless an excludable resource. Unlike with air, owners and controllers have the capacity to restrict access to data under various conditions, monetary (e.g. subscription, license) or not (e.g. club membership). Yet, due to easy replication and distribution through the internet, once data has been released publicly, voluntarily or not (e.g. leaks), it becomes de facto non-excludable. In some cases, attempting to remove it may even draw more attention to it (i.e. the Streisand Effect)[9]. Finally, data, as information in digital form, is more easily discoverable, which considerably transforms risk factors.

[8] Weber, S. (2004), *The Success of Open Source*, Harvard University Press.

[9] Hagenbach, J. and F. Koessler, "The Streisand effect: Signaling and partial sophistication", *Journal of Economic Behavior & Organization*, Volume 143, 2017, Pages 1-8, https://doi.org/10.1016/j.jebo.2017.09.001.

There are many ways to generate value in the data-driven economy

Value can be generated from data in ways similar to other assets, in particular by aggregating it and monopolizing access (in bulk or through APIs) in order to monetize it. More importantly, businesses can use data analysis tools to better understand their activity history, anticipate trends, monitor operations or prepare decisions through so-called descriptive, predictive, diagnostic and prescriptive analytics, respectively. For consumers and the general public, respectful data collection and processing can mean increased value through personalization of services.

While material resources are consumed in the production value chain of physical goods (e.g. refining oil into fuels, or combining elements in chemistry), data value chains function differently. The non-rival, replicable and durable nature of data enables the same data set to be shared or recombined in several concomitant value chains, the outcomes of which can be useful for a multitude of ultimate beneficiaries. In other words, data can be re-exploited infinitely at low marginal costs. It is data infrastructure and analytics that are the primary costs related to data re-use.

Data value chains are highly non linear

At the most basic level, if two actors possess one picture each and freely share it with each other, both end up with two pictures. In this case, the resulting total amount of pictures among them is 4 instead of the initial 2. In other terms: 1 + 1 = 4, an expansion of value that is compounded as sharing is reiterated. The shareability of data is thus a critical contributor to the creation of value.

A very small amount of data (e.g. password or encryption key) can also unlock the potential of an extremely valuable but locked data set. Moreover, when numerous data units are aggregated, the value of the result is often vastly higher than the sum of the parts. This is especially true if the result is made available to a broad audience beyond the initial contributors or if further analysis allows for the detection of meaningful patterns or insights.

More importantly, two data sets, useless on their own but highly complementary, can become immensely valuable if properly combined (e.g. a list of individuals and a separate list of their consumption habits, both encoded with matching neutral identifiers). Conversely, combining two databases can totally destroy the value of the resulting set if one is extremely accurate but the other corrupted. In the strange data economy, 1 + 1 can equal 4, much more, or much less, depending on the circumstances. This raises new questions regarding the distribution of the created value among actors.

Important positive and negative externalities

In economic literature, an externality is a cost or benefit that is imposed on a third party that did not agree to incur that cost or benefit. It can be positive or negative, and incorporate private and/or social costs or benefits.[10] For data, it is relevant in many regards, touching upon the combination – and potential balancing – of social and economic value creation. Examples of positive externalities include: the optimization of manufacturing processes reducing pollution or information mutualization efforts like Wikipedia, benefiting the broader public beyond the contributors. On the other hand, although hyperscale data centers become more efficient, it is important to consider the environmental impact of the energy demands from the digital economy.[11] Likewise, disinformation and political polarization can also be considered examples of negative externalities in the data age.

Positive externalities around data are often difficult to measure and thus overlooked, particularly when of a non-monetary nature (e.g. the availability of free search engines or videoconferencing tools). The same goes for opportunity costs due to the restricted availability of proprietary data that could otherwise be useful for development (e.g. agricultural data). Identifying such externalities should be a major aspect of the debate on data.

[10] Pigou, A. C. (2002), *The Economics of Welfare*, Routledge.

[11] IEA (2020), "Data Centres and Data Transmission Networks", *Tracking Report*, June 2020, www.iea.org/reports/data-centres-and-data-transmission-networks.

Quotes from consulted stakeholders

The value of data is not always intrinsic. It changes according to context, who uses it, what it is used for and what it is combined with.

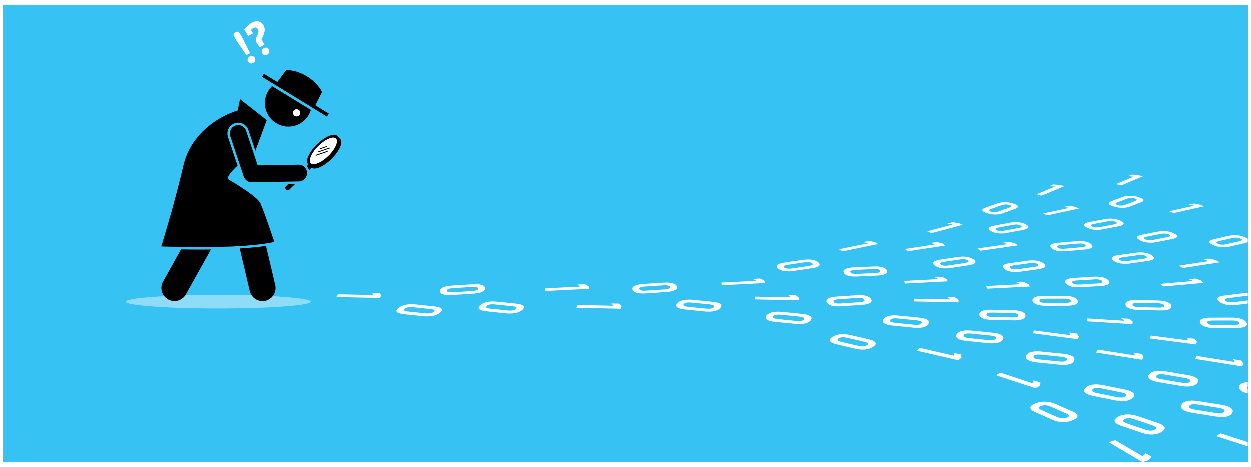
Data is different because it is generative. Using it creates more data and more value.

Data cannot be owned, but it can be sold.

Data has no value if you cannot make use of it. In some ways it can also be a burden. It depends on what use you can make of it. If you were to take all the data from a big tech, for example, you would not have the resources or the skills or tech equipment to deal with it.

A chunk of 0s and 1s might not tell you anything if you don't have the tools to analyze or decode them.

LOCATION OF STORAGE AND PROCESSING **IS NOT ALL THAT MATTERS**



Who collects, processes or accesses data - and for what purpose(s) - is of high relevance.

Location of storage and processing is only one part of the picture

Data is created, collected, stored, processed, accessed, used and also destroyed in numerous geographic locations. Yet, political discourse about data tends to focus on only two of these components: the location of storage and processing. The tangible reality of massive data centers triggers familiar images of vaults (where data is hoarded) or factories (where data is processed). As usual, while the analogies hold some truth, they are limiting.

In a context where cloud services have proliferated worldwide[12], the actual location of data can be hard to determine, sometimes by design. Not only is it moved at the speed of light along its processing workflow, but it can be replicated in diverse locations for reasons of security (e.g. geo redundancy) or efficiency (e.g. content delivery networks). It can also be split in many different and distributed pieces (e.g. sharding) to facilitate processing. Technical measures can potentially enable specific data to be stored and processed in a particular geography, if explicitly requested by the corresponding data controller or decided by the data processor for optimization. This, however, is not simple, and can be onerous and difficult to achieve. Major cloud providers distribute data centers around the world in several locations, the choice of which depends on a combination of factors including cheap and renewable energy sources, risks of natural disasters, quality of connectivity, amenable local climate, and predictable regulatory environment.

More importantly regarding processing, there have been significant evolutions in the management of data. Cloud services have become much more complex than providing storage or historic hosting of web pages; enterprise servers have migrated to public clouds; and edge computing and real-time processing have significantly developed, in particular regarding data from IoT and other connected devices. Moreover, a proportion of data is also directly processed in distributed devices themselves. Regulatory frameworks related to data need to be sufficiently future-proof to accommodate these rapid and ongoing evolutions. As described below, other factors than location of storage and processing seem more relevant and useful in that regard.

[12] Despite the decline in prices and expansion in cloud services offers, it should be noted that these services are not yet universal, as substantive connectivity gaps to enable them persist. See: ITU and Unesco (2020), *State of Broadband Report* 2020, www.broadbandcommission.org/publication/the-state-of-broadband-2020.

Who collects or processes data, from whom and for whom, is highly relevant

Where and from whom is data collected? There are numerous avenues to do so, be it for personal or non-personal data. It can be collected through proliferating connected devices that generate a vast volume and streams of data from and for a multitude of sectors (e.g. industry, health, mobility, finance, etc). Collection can also result from an explicit request to or implicit tracking of customers or users of a service, producing personally identifiable or non-identifiable data. Finally, individuals and entities, particularly in the age of social media, voluntarily upload, publicly or privately, vast amounts of content online for global distribution.

Other important factors are: who actually collects such data, who processes it (in what can be long and complex value chains), who has access to it along the way, and who ultimately receives the outcomes of such processing. Each of these actors, again, can be located in different countries.

These numerous geographic connection factors (nexus) imply a multiplicity of potentially applicable laws. As a result, the mere location of storage or processing is hardly sufficient as a basis for regulatory purposes, including because the value created can be manifested elsewhere. An exclusive focus on those criteria may actually lead to unintended consequences, particularly when data localization measures are implemented (i.e. laws or regulations requiring data generated in a country to be stored on servers physically located within that country), as discussed below.

Purpose and use are key

Data is the lifeblood of societies and economies. It can be leveraged for research, to monitor infrastructures, industrial plants or the environment, for individual communication and expression or for entertainment, for marketing and sales, including through behavioral targeting, and in almost any human activity, for profit or not. Data collected for one purpose can be re-used with amazingly positive benefits, yet unauthorized re-use can have very negative consequences, as revealed in 2018 in the case of Cambridge Analytica.

Conditions of collection, access, sharing and use of data must match the purpose of the processing. Ethical dimensions must be taken into account regarding purposes and algorithmic processing, in a way similar to the debates pertaining to bioengineering. In this context, the traceability of data sharing and access becomes a major issue, as is ensuring the integrity of data along value chains. New questions regarding stewardship of data and the rights of individuals and entities regarding their own data are coming to the forefront of policy debates.

People increasingly focus on data centers, perceived as vaults where data is processed – a sort of mental extension of the simple racks of web servers of hosting providers. Just a larger number of them. However, here *more* is also *different*: the growing complexity of services provided in the cloud and of data value chains brings new and difficult policy challenges.

As mentioned above, technical challenges are substantial when attempting to separate different types of data. In this context, a useful distinction can be introduced between "data at rest" (i.e. storage) "in transit" (i.e. data flows) and "in action" (i.e., its use).[13]

[13] Bergé, J. S., S. Grumbach and V. Zeno-Zencovich, (2018), "The 'Datasphere', Data Flows Beyond Control, and the Challenges for Law and Governance" *European Journal of Comparative Law and Governance*, Vol. 5, Issue 2, https://ssrn.com/abstract=3185943.

Quotes from consulted stakeholders

For most companies, the data they create internally, algorithms and data processes are extremely interlinked. They are not so easily transposable.

It's terribly tempting to run around doing classification of things. When you know how to define different kinds of data, then claim that we should control that type of data and in which way. However, its uses are almost certainly the big issue here, and agreeing on what uses are permitted and which ones are not is crucial for an agreement about dealing with cross-border data flows.

Locations matter, but not in terms of what servers data is located in. It is more about the context than location. It is context that gives meaning to the data.

Thinking about data in terms of server location is an old-fashioned conception of what the web was thirty years ago. There are recent technology innovations, such as edge-based technologies, virtualization, tokenization of data, etc. Those are all non-traditional client-server relationships. We need to think about data in its native sense. It could be in a server at some point along the way, but there are other places it could be stored and maintained.

We need to put the edge at the center. How can we allow this data to flow in a way that improves people's lives.

How data is used matters, maybe more than the typology [of data] itself.

Location does matter when governments want to coerce or prosecute IT companies. If a company has a data center in-country, then law enforcement can arrest employees (or subcontractors).

The data warehouse question is sometimes a bit of a red herring for the political economy issues that are really behind it. Very few countries have the infrastructure, the capacity, and even the electricity and power to have these.

Where data is stored need not or should not govern how your data is used by whom and for what purpose.

We need to generate a clear understanding of data handling obligations, regardless of who and where, and to focus on economic development. We really need to move away from this idea that physical location has to govern everything.

CHAPTER

2

ON FREE FLOW OF DATA

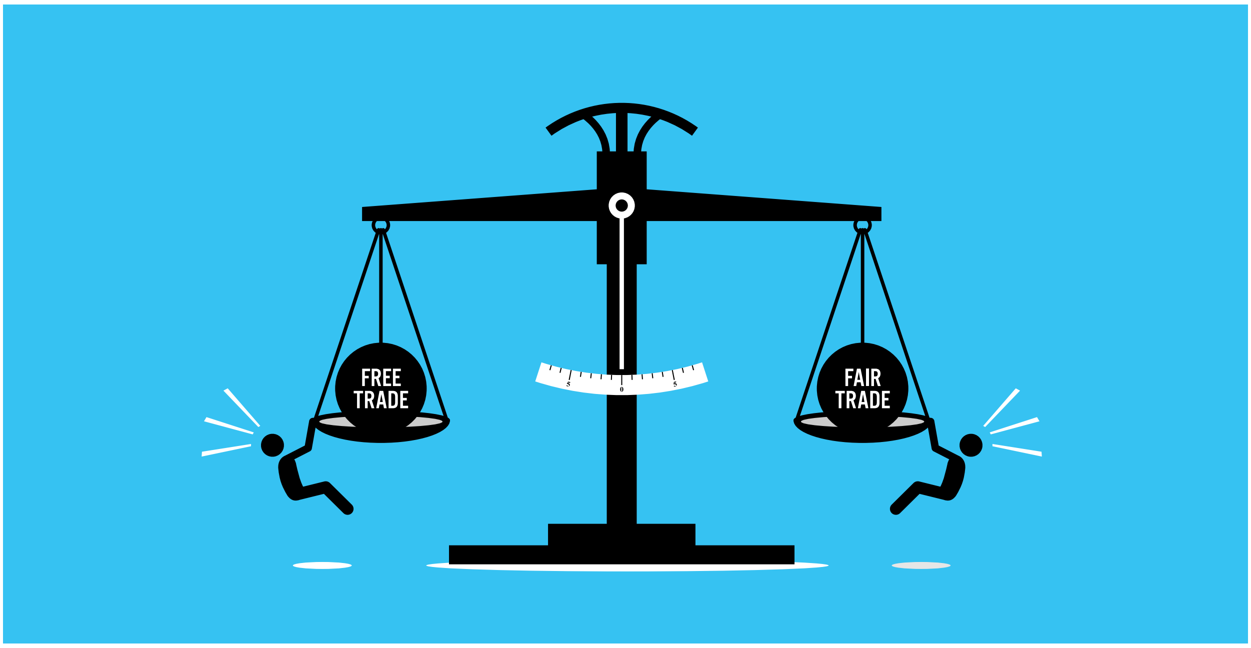
> *By continuing to address challenges related to privacy, data protection, intellectual property rights, and security, we can further facilitate data free flow and strengthen consumer and business trust.*

G20 MINISTERIAL STATEMENT ON TRADE AND DIGITAL ECONOMY

JUNE 8, 2019

- *The shadow of the free trade debate*
- *Free Flow of Data is a topic high on global policy agendas*
- *Concerns exist regarding digital interdependence dynamics*
- *Cross-border Data Flows depend upon trust*

THE SHADOW OF THE FREE TRADE DEBATE



Discussions around Free Flow of Data are strongly influenced by existing tensions around free trade.

Free trade is historically advocated to maximize the "Wealth of Nations"

In the 17th and 18th centuries, the dominant mercantilist philosophy considered that, to increase their wealth, countries should export more than they import, the trade surplus allowing to expand their treasure (e.g. accumulating gold and silver). In a context of growing dynamism and industrial revolution, Adam Smith challenged that notion in his 1776 seminal work "The Wealth of Nations" and argued strongly for countries to specialize in what they were best at producing (absolute advantage), also advocating for less government involvement and a reduction of barriers to trade.

A few years later, David Ricardo offered a fundamentally new perspective, showing that what mattered for mutual benefits from trade was simply for a country to be relatively more efficient in producing something over another (comparative advantage). Hence, the theory of international trade was developed. A central argument is that international competition stimulates greater innovation and productivity, benefiting consumers with better products at lower prices, while the opposing force of protectionism can hinder progress. In other words, free trade generates wealth.

Complex frameworks are still required to reduce barriers to trade

In order to reduce barriers to trade, countries engage in bilateral or multilateral arrangements. Such agreements consist of complex frameworks, dealing not only with clauses to reduce (or eliminate) tariffs, but also provisions on trade quotas, taxes, investment guarantees, intellectual property, labour, services, etc. Key objectives settle on a common vocabulary between trading partners, to make misunderstandings less likely, and to balance obligations or benefits. Therefore, taxonomies are key for international trade lawyers and negotiators.

Moreover, trade agreements aim to foster trust (i.e. minimizing risk, increasing confidence, reducing mistrust) and expectations for long-term cooperation, by establishing procedures for monitoring compliance, detecting any direct or disguised attempts at creating trade barriers, and punishing violations.

Global value chains trigger interdependence

The classic international trade model was developed with goods at the center, assuming that factors of production (e.g. labor, capital, and technology) were fixed and that services were non-tradable. Globalization and technological development, however, have enabled services, capital, investment and labour to now flow over national borders. Liberalization of telecommunication services also facilitated the creation of new business models and further accelerated interconnectedness of cross-border flows of goods and services.

The emergence of global value chains has also meant that for many products components are brought together from different countries and that the traditional rule of “country of origin” no longer applies as simply. It also impacts how certain companies see themselves, as global rather than national firms, selling and procuring materials and services around the world. This is even more true for purely digital companies, which can technically serve customers globally from the onset.

A backlash triggered by socio-economic dynamics

The dynamics of interdependence have also meant that states – and public opinion – are more and more concerned with the perceived imbalances and negative externalities of international trade. A form of backlash is triggered inter alia by fears related to trade deficits and fairness; domestic impacts of outsourcing; the concern that trade deals benefit larger corporations more than smaller firms, or that domestic producers can be squeezed out by foreign rivals with huge economies of scale or lower labor or environmental standards.

Debates around trade agreements can be highly contentious. They involve reconciling different sectoral interests and policy objectives. At stake is the dynamic distribution of gains and losses not only among countries, but also within countries, between economic sectors and between individuals. The history of trade is thus marked by cycles of openness and protectionism measures, be the economic (e.g. protecting domestic employment, domestic consumers and infant industries) or related to states' national security and political stability. In this regard, the current international environment, ongoing negotiations of several agreements notwithstanding, is marked by geopolitical tensions, a reduction in trust and several trade wars. This casts some negative shadow on debates about Free Flow of Data.

Quotes from consulted stakeholders

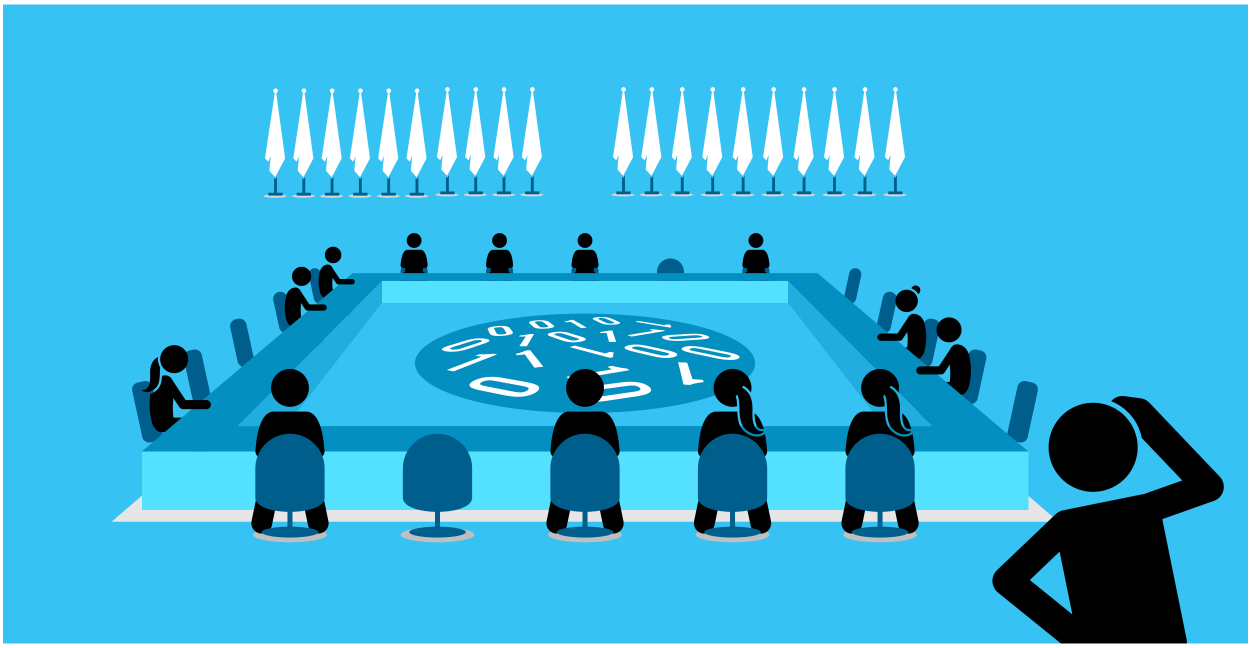
The whole argument behind Data Sovereignty is that a government needs to control something going on within its territory. That's an anathema to international trade because that's about governments accepting imports of goods and services from around the world.

Do we have to select a Chinese approach or an American or Indian approach, only to find ourselves in a position as during the Cold War where we have to be aligned with one or the other? This is not good for digital cooperation. That is not how we will continue to promote innovation and economic development.

Data Sovereignty is an attempt in Europe, for example, to have national champions. In South Africa and India it is a rationale for trade protectionism. I think that it has become a buzzword to justify both varieties of things, for which there are perfectly good solutions. So sovereignty is being misused in the proper sense of international law. It is, of course, very political.

We should explore a way forward for talking about Data Sovereignty which is respectful of a country's rights to govern and trade in a fair and equitable way. The global data infrastructure and the economies of scale are pushing towards a lot of competition issues that are unfair to some of the developing countries.

FREE FLOW OF DATA IS HIGH **ON GLOBAL POLICY AGENDAS**



Cross-border data flows are a direct result of the internet architecture, but remain difficult to address in existing multilateral fora.

The technical default on the internet

Data flowing freely across borders is intrinsic to the decentralized architecture of the internet. Its very purpose is to connect any device, network or computer respecting its protocols, irrespective of their location. The non-geographic nature of the network further means that data transfer paths between autonomous systems follow topological and not geographic parameters. The internet, which is the underlying infrastructure enabling all the applications and services built upon it, is entirely about data flows and generally conceived as agnostic to the content of the packets transported. The multiplication of connections and peering arrangements contributes to the overall resilience and security of the whole network, beneficial to all.

Cross-border flow of goods can be controlled at customs and physical points of entry. Controlling data flows is however a more complex challenge, and tampering with the internet architecture by reimposing geographic criteria can impact its proper functioning.

Nevertheless, some countries have imposed a limitation of the number of gateways, and when the political will exists various technical solutions have been introduced (e.g. geo-blocking, deep packet inspections, filtering), making it easier than before to control data flows. Encryption however adds a layer of complexity to the issue.

Intense international policy debates about Free Flow of Data

As data becomes more easily discoverable, concerns around data protection have set the tone of international debates around data flows, even before it became a trade issue.

Debates regarding Free Flow of Data started in the 70's around privacy concerns, leading to first intergovernmental outcomes in 1980 with the Organisation for Economic Cooperation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data[14], and in 1981, with the Council of Europe's Convention 108. Since then, privacy has remained a major topic on the international agenda. Asia Pacific Economic Cooperation (APEC), for example, agreed in 2005 to a Privacy Framework (updated in 2011 with the APEC Cross-Border Privacy Rules). Similarly, the EU with its General Data Protection Regulation (GDPR), which entered into force in 2018, established an extensive approach that has influenced a number of non-EU states to adopt similar measures (e.g. Argentina, Israel, New Zealand, Uruguay). The Association of Southeast Asian Nations (ASEAN) Framework for Personal Data Protection and the African Union Convention on Cybersecurity and Personal Data Protection (not yet in force) are other examples of international agreements in this field .

The issue of data flows has not ceased permeating international fora, in the background of more general discussions on digitalization. In Latin America, regional discussions around Free Flow of Data have informed a broader debate on the opportunities and challenges of a digital single market for the region – as a tool to counter the issue of lack of harmonization of rules and standards.[16] In the EU, a regulation aiming to ensure free flow of non-personal data[17], albeit only among its members, became applicable in 2019. Significatively, the Declaration of G-20 Leaders[18] in 2019 endorsed the notion of "Data Free Flow with Trust" (DFFT) promoted by Japan.

Notwithstanding such declarations and efforts, large divergences remain among states, in particular given the adoption (or intention thereof) by several countries of various data localization provisions. Likewise, the 2020 decision of the Court of Justice of the European Union (CJEU) invalidating the Privacy Shield illustrated the difficulty of establishing interoperability between very different privacy regimes.

A difficult integration in traditional trade negotiations

Policy makers have been attempting for many years to agree on a common vocabulary and a set of rules to integrate data flows within trade frameworks. The 1995 World Trade Organization (WTO) General Agreement on Trade in Services (GATS) is the most comprehensive multilateral framework so far, with chapters on telecommunications, computing and financial services, which explicitly mention privacy as a potential exception to its provisions. Yet, since its entering into force, the GATS is recognized to have become largely insufficient in light of the proliferation of digital products and services. In 1997, the United States proposal of the "Framework for Global Electronic Commerce" inaugurated a new direction of international negotiations around trade and technology. The Framework was important, as it led to principles, which were eventually included in bilateral agreements.[19]

[14] First revised in 2013 and currently again under revision.

[15] European Parliament (2016), "General Data Protection Regulation", *Official Journal of the European Union* https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[16] Economic Commission for Latin America and the Caribbean and Internet & Jurisdiction Policy Network (2020), *Regional Status Report*, www.internetjurisdiction.net/news/release-of-internet-jurisdiction-and-eclac-regional-status-report-2020

[17] European Parliament (2018), "Framework for the Free Flow of Non-Personal Data", *Official Journal of the European Union*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R1807.

[18] G20 (2019), G20 *Osaka Leaders' Declaration*, https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/en/documents/final_g20_osaka_leaders_declaration.html.

[19] United States (1997), "Framework for Global Electronic Commerce", *White House archive*, https://clintonwhitehouse4.archives.gov/WH/New/Commerce/about.html.

However, despite attempts to expand and clarify WTO rules on the issue, including through dedicated work programs and joint statements on e-commerce, little advancement has been made.[20] No consensus has been reached to date at the WTO on the difference between e-commerce and digital trade, nor on defining data and data flows.

Given the difficulty of reaching a broad agreement on e-commerce and digital trade, several regional, multilateral and bilateral Free Trade Agreements (FTA) have emerged. E-commerce chapters appear in FTAs by Australia, Canada, the European Union and the United States, some of which have been progressively renamed digital trade chapters. The first FTAs to include a binding clause on cross-border data flows have been the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the United States Mexico–Canada Agreement (USMCA). In both, exceptions are accepted to achieve domestic policy objectives (i.e. national security, public morals and privacy) as long as done in the least trade distorting manner possible. Recent examples of FTAs taking the matter of digital trade even further are the Digital Economy Partnership Agreement (DEPA)[21] between Singapore, Chile and New Zealand and the Australia-Singapore Digital Economy Agreement (DEA).[22] These agreements address broad digital issues such as AI, distributed ledger technology, smart cities, digital identities, e-payments, e-invoicing, IoT, data protection and privacy, data portability, data innovation and regulatory sandboxes for cross-border data transfers.

Despite advances in a select number of FTAs, important divergences continue to exist among major state powers.[23] The United States and the European Union continue to have sharply different regimes, not necessarily interoperable, while China does not bind itself by any rules regarding Free Flow of Data. These contrasts were prominently on display at the Osaka 2019 G-20 meeting, both on substance, regarding data localization measures, and on process, regarding whether the sole negotiation venue should be the WTO or not, given the abundance of parallel regimes (e.g. privacy, taxation, law enforcement, content moderation and platform regulation). In this regard, developing countries are still lagging behind in understanding how to position themselves in the digital trade debate, given the substantive information asymmetries and lack of an established framework for measuring the value of data.[24]

Measuring actual value flows is particularly difficult

The absence of centralized points of control on the internet makes it difficult to measure the exponential volume of global traffic. Likewise, the international dispersion of data collection, processing, storage, and use challenges the measurement of stocks and flows of data. This is true in terms of volume, but even more so regarding economic value, let alone social value. Proper taxonomies and measurement methodologies are clearly needed but no easy consensus seems achievable.[25] This has non-trivial implications not only for the accuracy of national and international statistics but also for the development of evidence-based policies, the assessment of the role of data for businesses, and for the understanding of the effects of data for individual and social well being.

Considerable efforts need to be made both in terms of producing national-level statistics and coordinating to develop international standards for measuring data and the value it produces.

[20] A proposal to create a "Trade in Services Agreement" was never achieved. See WTO (n.d.), "E-commerce", WTO *website*, https://www.wto.org/english/tratop_e/ecom_e/ecom_e.htm.

[21] MIT (2020), *Digital Economy Partnership Agreement*, Ministry of Trade and Industry of Singapore, https://www.mti.gov.sg/Improving-Trade/Digital-Economy-Agreements/The-Digital-Economy-Partnership-Agreement.

[22] DFAT (2020), *Australia-Singapore Digital Economy Agreement*, Department of Foreign Affairs of Australia, https://www.dfat.gov.au/trade/services-and-digital-trade/australia-and-singapore-digital-economy-agreement.

[23] Aaronson, S. (2018), "Data Is Different: Why the World Needs a New Approach to Governing Cross-border Data Flows", CIGI *Paper Series*, No. 197, www.cigionline.org/publications/data-different-why-world-needs-new-approach-governing-cross-border-data-flows. Ciuriak, D. and M.

[24] Ptashkina (2019), "Leveraging Digital Transformation for Development: A Global South Strategy for the Digital Economy", CIGI *Policy Brief*, No. 148, April, www.cigionline.org/publications/leveraging-digital-transformation-development-global-south-strategy-data-driven.

[25] OECD (2019), Measuring the Digital Transformation: A Roadmap for the Future, 2019, www.oecd.org/publications/measuring-the-digital-transformation-9789264311992-en.html.

Quotes from consulted stakeholders

The concept of free flow of information has become like a joker in a game that you can use in any circumstance. What originated as a means to an end, now has become an end in itself.

The starting point can be free flows and then restrictions, rather than restrictions on flows with some exceptions.

There is a major land-grab in terms of data.

One of the worries is making sure the discussion about the Free Flow of Data is really technically proficient. The other is that we talk about being able to keep data in just one country, as though the global internet is not a globally connected network.

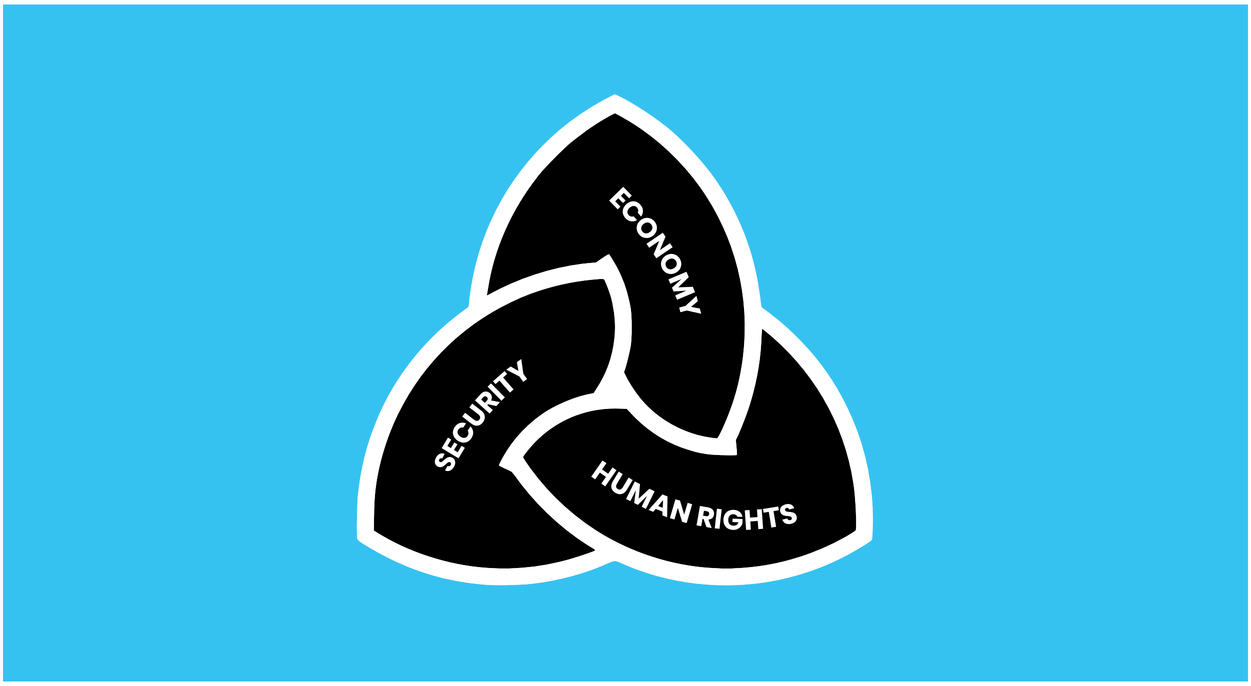
Data flows is most often a lever for compelling compliance with laws and regulations.

We should not be using privacy as the basis for restricting or allowing data flows. Privacy and data security protections should apply, no matter where data is stored and no matter how it's transferred. In fact, restricting data flows is a bad lever for ensuring privacy protections.

The point of reducing the excesses of free data flows is being elevated in the international agenda. Politicians play with customers' perception and elevate this pitch at a state level - to do something against the "evil companies", be they Chinese or American.

There are complementary concepts such as data solidarity, for example, that are underresearched. At this moment in time, there is an argument that can be made that you can only address these big societal challenges when we actually unlock the value behind data to create new insights. Isn't there an ethical obligation, for instance in some contexts, to share data based on a notion of solidarity? I don't think it is mutually exclusive to think about solidarity and data privacy, but the issue is that they have been treated very unequally.

CONCERNS EXIST REGARDING DIGITAL **INTERDEPENDENCE DYNAMICS**



Cross-border data flows raise various concerns, with overlapping security, economic and human rights dimensions.

Faster dynamics of interdependence for data

Interdependence is a well-known feature of the global international landscape. It involves not only the interconnection between states and among different actors, but also interrelations between sectors and policy areas. In the offline world, issues related to economy, security and human rights are often systemically interlinked in such ways that one recurrently affects the conditions or the desired outcomes in another.

Yet, these systemic aspects are even more complex in the digital era. The main difference comes from the properties of big data, particularly volume, velocity and variety. The enormous volume of data brings qualitative changes to economic and social dynamics. The speed at which data flows results in an acceleration of its effects in all policy dimensions. This, in addition, involves a broad variety of stakeholders concomitantly and turns up the volume of the impact, which may be felt by millions of people at once. Typical of a cascading effect, concerns related to the Free Flow of Data engage a multitude of involved parties and agendas – some of them more prominent than others. These concerns can be described according to their main relevance to: security, economy and human rights.

Security concerns

Concerns around free flows of data may be based on security aspects, both in terms of physical and digital security, as these are increasingly intertwined. Moreover, states may wish to protect data considered sensitive, including government data, strategic and defense data, against foreign surveillance. To ensure security and stability, states want to be able to control, and retain exclusive access to that data at all times. Furthermore, states want to ensure that they and their law enforcement authorities have appropriate access to the data they need to ensure national security and conduct criminal investigations (electronic evidence), but they may not have access to it when it is not under their jurisdiction except through cumbersome Mutual Legal Assistance mechanisms or opaque stealth access[26]. Finally, the notion of strategic autonomy aims to minimize dependency on digital infrastructures and services procured or controlled by foreign entities that may directly or indirectly be subject to the authority of a foreign state. This also applies to prevention of economic espionage.

Economic concerns

Regarding economic dynamics, the current geographic distribution of the dominant players of the digital economy raises fears in many actors (states, companies and citizens) of being left behind in an international technological competition critical for the future, of losing jobs to outsourcing, and of being unable to catch up and create national champions because of lock-in effects. Additional worries stem from perceived anticompetitive practices by major actors.

Another key concern regards the distribution of the value created by the data economy and the desire to maximize and retain this economic value at the national level. A country expects to fairly benefit from the wealth generated by data from its citizens and companies, as opposed to that data ‘leaving’ the country or generating wealth elsewhere for other actors. The tense debate on taxation rules for data-driven companies both reveals and intensifies this concern.

Human rights and broader societal concerns

At a general level, concerns can also be distinguished through their relation to human rights and sociopolitical dimensions. For the former, the objectives pursued are those of promoting inclusion and ending discrimination (e.g. the UN 2030 Agenda value of “leaving no one behind”)[27] and protecting digital rights (e.g. right to privacy, freedom of expression and of having access to the internet). Given the intense activity on social media and the proliferation of connected devices (e.g. phones and IoT appliances), the volume of available personal data has grown exponentially, increasing risks and abuses, and leading to important concerns related to privacy and data protection.

Moreover, while low technical barriers for online expression have facilitated free speech around the world, sociopolitical concerns have also emerged. These relate to increased levels of state and corporate surveillance and control, and also to the online spread of harassment, hate, disinformation and even terrorist propaganda, including across borders. Although extremely limited in terms of proportion (less than 0,2% on a platform like Facebook[28]), the sheer absolute volume of such illegal or harmful content makes this a very legitimate and visible societal problem. This triggers calls for restrictive policy actions in a context of high uncertainty over the applicability of national laws beyond national territories.

Finally, the role of behavioral targeting and algorithmic recommendations in generating political polarisation and propagating disinformation triggers growing concerns regarding the impact on public opinion and the democratic process, and ultimately, the cohesion of societies.

[26] European Parliament (2017), “Legal Framework for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices”, *Study for the LIBE Committee*, www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf.

[27] United Nations (2020). “Leave No One Behind”, *United Nations Sustainable Development Group website*, https://unsdg.un.org/2030-agenda/universal-values/leave-no-one-behind .

[28] Facebook (2020), *Facebook Transparency Report*, https://transparency.facebook.com.

Speed of adaptation is a concern in itself

The dynamics of the interdependent data economy are much more rapid than those of traditional trade. Although an earlier awareness of emerging problems is facilitated, this creates a particular challenge for the drafting and adoption of the necessary legal frameworks to address the concerns described above. Time pressure coupled with political constraints weigh on the law-making process, often leading to frantic legal patching in an uncoordinated manner.[29]

Quotes from consulted stakeholders

We keep thinking that what is digital is so different. But we had similar problems before.

Of course we want to promote Free Flow of Data, but we do not want to be naïve.

There is no guarantee that the physical security provided is better domestically than out of the country. Cloud providers may implement physical security better than governments.

Restrictive measures are likely to stifle potential for innovations and new discoveries across borders. It may limit free flow of information and may undermine access to information as a human rights principle.

Countries are concerned about content and the impact that that content has on their citizens.

The concerns that we are seeing around data flows now are only the tip of the iceberg.

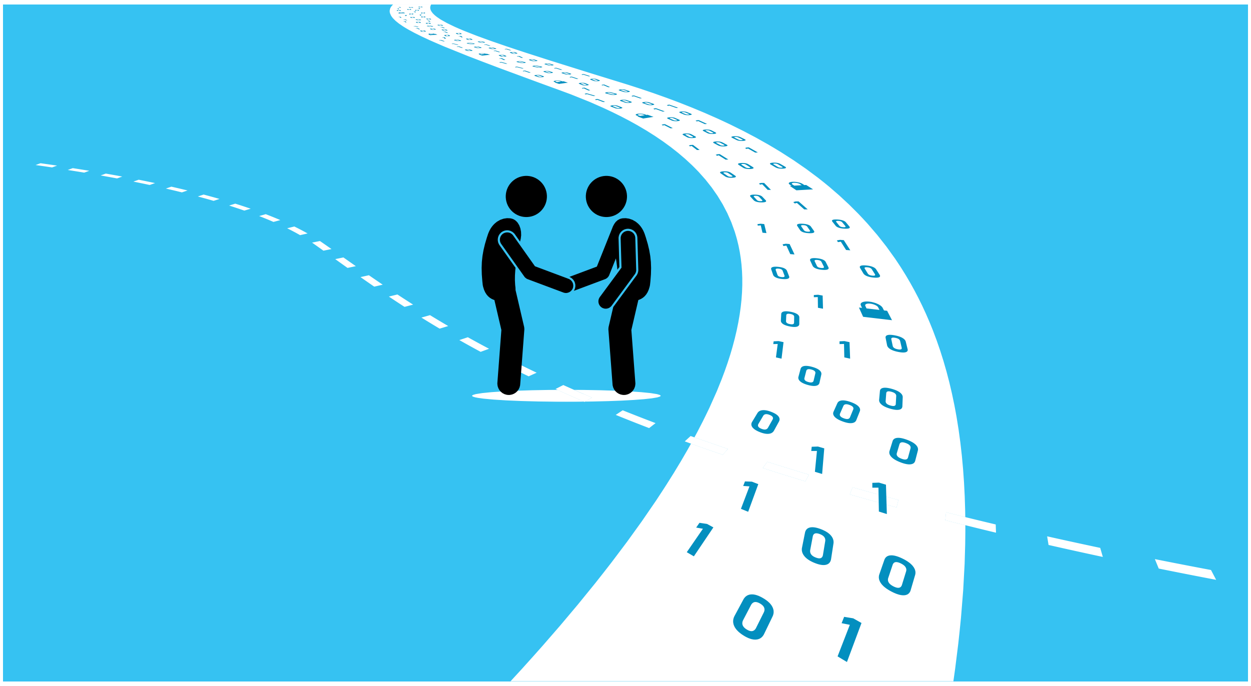
We want to make sure that our human rights flow with our data.

Key challenges for the governance of data flows include who sets, implements and enforces the rules.

The whole discussion around sovereignty affects things that go much beyond digital services.

[29] Internet & Jurisdiction Policy Network (2019), *Global Status Report* 2019, www.internetjurisdiction.net/news/release-of-internet-jurisdiction-and-eclac-regional-status-report-2020.

CROSS-BORDER DATA FLOWS **DEPEND UPON TRUST**



Dealing with potential misuses of data while preserving its free technical transit requires dedicated trust-building frameworks.

Building trust and responsibility around (mis-)uses

The value of data is maximized when it is flowing and used with trust across borders and sectors. Addressing the concerns described above to establish trust in data flows can be approached in many ways. Security measures by the various operators can ensure transmission quality and integrity of "data in transit"[30]. Regimes according to types of data (e.g. personal or not, with or without special legal protection, or sector-based) are possible but are confronted with reuse across sectors, a lack of clearly agreed taxonomies and the difficulty to tag every piece of data. Separate regimes by type of problem or sector (e.g. privacy, taxation, health, defense, agriculture) are relevant but they require intense coordination within countries, among them and between siloed policy and regulatory communities, in order to prevent collateral impacts. Ensuring that protections travel with the data is also an important technical challenge.

In any case, the flows themselves are actually less at issue than what organizations (including states in the case of undue surveillance) and individuals can or cannot do with data and what impact this has, where, and on whom. Risk assessments and liability regimes regarding mis-uses and behaviors can be a more promising avenue, notwithstanding the difficulty to find solutions for cross-border compliance and enforcement.

[30] For the distinction between data at rest (i.e., storage), in transit (i.e., data flows) and in action (i.e., use) – see: Bergé, J. S., and S. Grumbach and V. Zeno-Zencovich (2018), "The 'Datasphere', Data Flows Beyond Control, and the Challenges for Law and Governance", *European Journal of Comparative Law and Governance*, Vol. 5, Issue 2, https://ssrn.com/abstract=3185943.

Preserving the default of free transit at the technical layer

As mentioned previously, data flowing freely across borders is a default characteristic of the non-geographic architecture of the internet. The end-to-end principle and the neutrality of the network as a transport layer are key reasons for its success and its generative quality, which enables the prodigious diversity of applications for both social and economic benefits.

Countries lacking sufficient communication or electrical infrastructures, or the required enabling environment (e.g. legal certainty, skilled labour, etc), critically depend upon accessing services (including cloud ones) based in other countries, as do many companies, large or small, for scaling up globally. Likewise, cross-border flows are essential for the exercise of freedom of expression and access to information, enshrined in Art 19 of the 1948 Universal Declaration of Human Rights, which, presciently, contained the expression "irrespective of borders".

Technically limiting data flows is an engineering issue and means have increasingly been developed to do so. Yet, blunt tinkering with the transport layer and routing makes a system everyone relies upon less resilient and thus vulnerable to attacks. Rather than trying to retrofit by force this unique infrastructure with the old paradigm of geographic frontiers, laws must deal with it in an innovative manner, as they did with previous technologies (e.g. regulations on airspace or outer space).

Exploring new, virtual borders

Agreements among a group of countries can create *virtual territories* of sorts enabling free flow of data amongst them. Outside countries or even individual operators, through certification (or adequacy), can be allowed to join and enjoy the same benefits. This is the approach of the European Union, but such virtual territories need not be geographically contiguous. This, however, demands among participants a degree of harmonization difficult to achieve: the tribulations around the Safe Harbor and the Privacy Shield illustrate the interoperability challenges in privacy protection even between the United States and the European Union. Additional frameworks interfacing different virtual territories would also be needed to enable scalability, in an architecture reminiscent of the complex mesh of trade agreements. Yet, smaller countries might be rapidly excluded.

Data spaces related to particular sectors can also be envisaged as part of the arrangements described above (as in the European Gaia-X initiative) or outside of them. Management of the complex interdependence between sectors will be the key question here, in order to avoid an excessive siloing that would reduce the opportunities for useful cross-fertilization.

A *layered architecture* could allow free data flows within the network of the enterprise data centers of a particular company, or within the proprietary infrastructure of major cloud providers, irrespective of the location of said data centers, in order to facilitate the optimization of services around the globe. Determination of jurisdiction could then be attached to the locus of incorporation of the operator and where data is "in action"[31].

Finally, and more innovatively, one can consider the entire collection of data collected or produced, stored or processed, analyzed or put to use as a new, immaterial and human-produced, "Datasphere", in addition to the lithosphere, the hydrosphere and the atmosphere used in natural sciences. For each of them, an innovative setup was ultimately adopted in law, defining graduated levels of authority for sovereign entities: exclusive, partial and shared (e.g. for outer space), as well as the rights of non-state actors (e.g. of a land owner regarding the air above it). A similar construction might be envisaged to organize the interfaces of physical territories (and sovereignties) with this Datasphere.

[31] See note 15 above.

Quotes from consulted stakeholders

There is no sufficient effort on trying to find convergence around the issues that create restrictions on data flows - either directly or indirectly.

This issue of Free Flow of Data is very important, because for some years we are trying to develop a digital regional market in Latin America. And one of the main issues is how to manage the data flows.

Free flows of Data and Data Sovereignty are the two sides of the same coin. What we want is Free Flow of Data with the appropriate protections.

It is incredible to think how much we are willing to spend because we distrust each other, as opposed to thinking about what is the role of government in facilitating the growth of trustworthy institutions.

Everyone agrees with the notion of trust. We can try to use this to anchor our discussion. The discussion now is very corrosive. We just need a small step of good-will so that we can move the discussion forward.

Perhaps we should move towards the direction of Free Flow of Data among trusted partners. We can try to achieve a framework of free flow of data among a certain number of countries. And then have rules for countries which are outside of this club - who can then be certified individually.

Sometimes to change the flow of information - you need a new institution or boost institutions.

The problem is that we think it can only be solved through a regulatory approach. Or a legislative approach. Or a litigation approach. Or an open source approach. It has to be all of those things at the same time. And they should be designed to work together. We need to frame this as an ecosystem approach.

If we weren't constrained by the geographic boundaries, we'd be able to achieve the engineering objectives more easily. We want to make connectivity as seamless as possible and to get everybody connected: when you can do things in a generic way, you have a much greater network effect than when you have to do something in a specialized way in each country.

CHAPTER

3

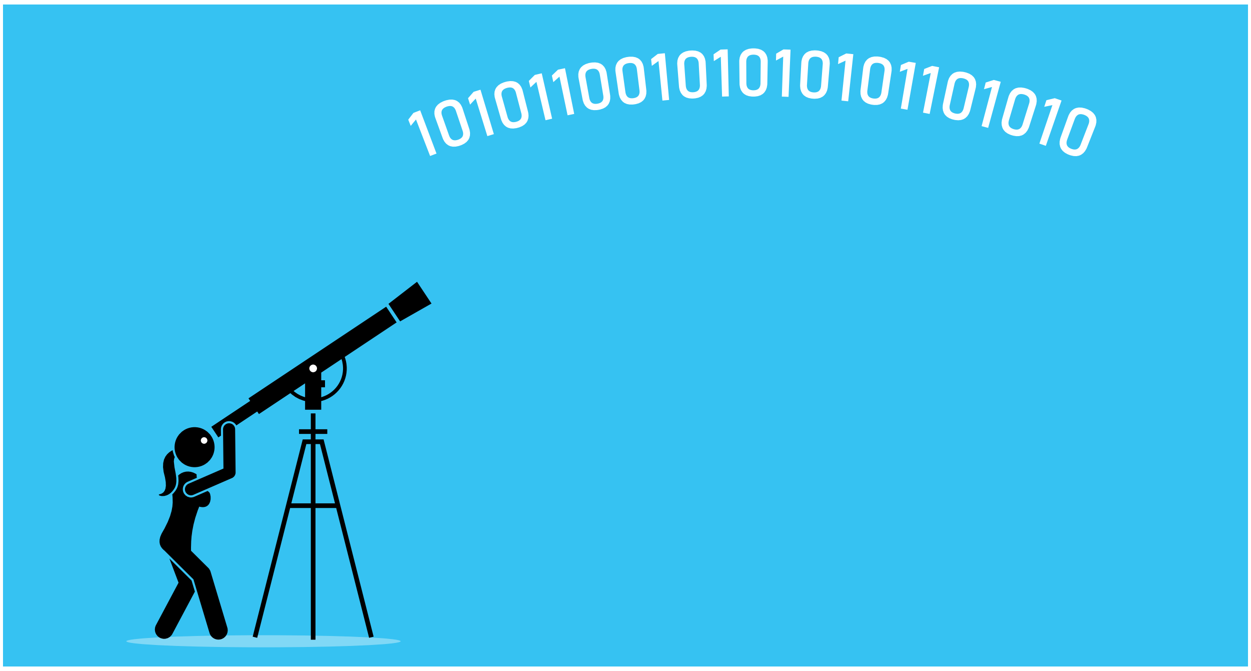
ON DATA SOVEREIGNTY

Managing the way that a large number of separate legal frameworks apply to the internet is one of the big policy challenges of our time and is more complex even than building the internet.

VINT CERF

- *Digital challenges to territorially-based sovereignty*
- *Data Sovereignty is peddled as a panacea to many concerns*
- *Implementation pitfalls*
- *Dealing with multiple jurisdictions*

DIGITAL CHALLENGES TO **TERRITORIALLY-BASED SOVEREIGNTY**



The non-geographic architecture of the internet is challenging the Westphalian paradigm underpinning our current international system.

The historic territorial nature of sovereignty

Unpacking the notion of Data Sovereignty first requires to recall the historic significance and powerful hold in the political discourse of the concept of sovereignty itself. It progressively emerged, particularly in Europe, through centuries of conflicts among power systems and intense philosophical and political debates, as attested by the writings of Jean Bodin, Grotius, Thomas Hobbes, John Locke, Montesquieu, or Rousseau.

Although many definitions exist and the concept is ripe with controversies regarding its implementation and basis, sovereignty is widely understood today as the *supreme authority of a state over a particular territory*. This also entails a responsibility to provide legal certainty and the protection of rights to different stakeholders within that territory.

The territorial basis of state sovereignty remains the foundational paradigm of modern states and numerous wars were fought to, inter alia, determine the precise boundaries of the exercise of state power and ensure the physical separation of the corresponding states.

The foundational principles of our international system

The Treaties of Westphalia, putting an end in 1648 to the European Thirty Years War, are usually credited for having enshrined the notion of territorial sovereignty in international law through the principle "*cujus regio, ejus religio*" (literally, "whose realm, their religion").

Yet, it is the creation of the United Nations in 1945 which, building on that basis, ultimately established the basis of the current international system through two fundamental principles. The first one is the "sovereign equality of states". The second one, important in the context of discussions on data, is the principle of "non-interference in the internal affairs of a sovereign state" ("*Par in parem imperium non habet*"), which highlights the separation and independence of national sovereignties.

Multi-level implementation and variations

These simple notions leave nonetheless room for multiple variations in their implementation.

First of all, many countries have internally adopted federal structures or recognized various levels of autonomy to portions of their territories (e.g. administrative regions) or of their populations (e.g. native communities), according to a hierarchical principle of subsidiarity.

Second, a wide range of bilateral or multilateral treaties adopted independently or under the auspices of international organizations, establish mutual commitments among states, limiting by mutual agreement the extent of their authority in specific areas. The integration process in the EU even sees member states "pool their sovereignties" by delegating some of their decision-making powers on specific matters to shared institutions. In addition, specific provisions apply to natural spaces adjacent to the state territory, including waters, air and space.

Finally, although still contested, new concepts have emerged like the "responsibility to protect" (an exception to the principle of non-interference to respond to massive human rights violations), or the "responsibility towards future generations" (in environmental issues).

The challenges brought by the digital age

The technical architecture of the internet was conceived as decentralized, cross-border and non-territorial from the onset. This transnational nature of the internet has generated unprecedented benefits for humankind, be they political, economic, cultural or social.

Yet, "because the internet is borderless, states are faced with the need to regulate conduct or subject matter in contexts where the territorial nexus is only partial and, in some cases, uncertain."[32] Moreover, sovereign decisions on internet matters from one state may, voluntarily or not, entail direct or indirect consequences on other territories, thereby somewhat infringing the sovereignty principle of non-interference.

More generally, the cross-border internet and its online spaces span a fragmented patchwork of national jurisdictions. As connectivity and internet penetration increase, so do legal conflicts, and traditional modes of legal cooperation struggle to resolve these tensions.

Like Galileo's telescope revealed the limits of the Ptolemaic vision of the universe, the internet is testing the limits of the classic Westphalian paradigm. The hierarchical intergovernmental system was suited to a world with few countries, clear separating frontiers and few cross-border interactions. It is challenged in complex digital societies, connected through cross-border online services, where transnational becomes the new normal and cooperation is required to manage common spaces.

[32] Kindred, H. M., T. Scassa, S. G. Coughlan and R. J. Currie (2014), *Law Beyond Borders: Extraterritorial Jurisdiction in an Age of Globalization*, Irwin Law.

The emergence of normative plurality

While states already struggle to enforce their national laws in cyberspace, the normative power of private entities becomes significant. Not only does the technical level of services set implicit norms (as coined in the expression "code is law" by Lawrence Lessig), but major platforms establish, implement and enforce their own rules through ever more detailed terms of service or community guidelines that apply to billions of users around the world.

Such rules not only cover the specific positioning of the service (e.g. no dog pictures on a platform for cat lovers) but increasingly – and ironically under the pressure of governments themselves – that normally are addressed by public order legislations.

In this context, traditional principles and approaches can become as much an obstacle as a solution to address the jurisdictional challenges of cross-border online spaces.

Quotes from consulted stakeholders

Sovereignty could potentially be viewed as a more flexible notion, and as a principle of international law that guides state interactions but does not dictate results.

Data Sovereignty is used by governments to express the dislike of seeing data going over their borders to generate value elsewhere, and not being usable or controllable within the country itself.

Data Sovereignty is actually more often used in the literature in the context of individuals than on a country level. The most common setting in which Data Sovereignty is discussed is in relation to indigenous populations.

We shouldn't just assume that everyone understands the term Data Sovereignty.

When people talk about sovereignty, they talk about control.

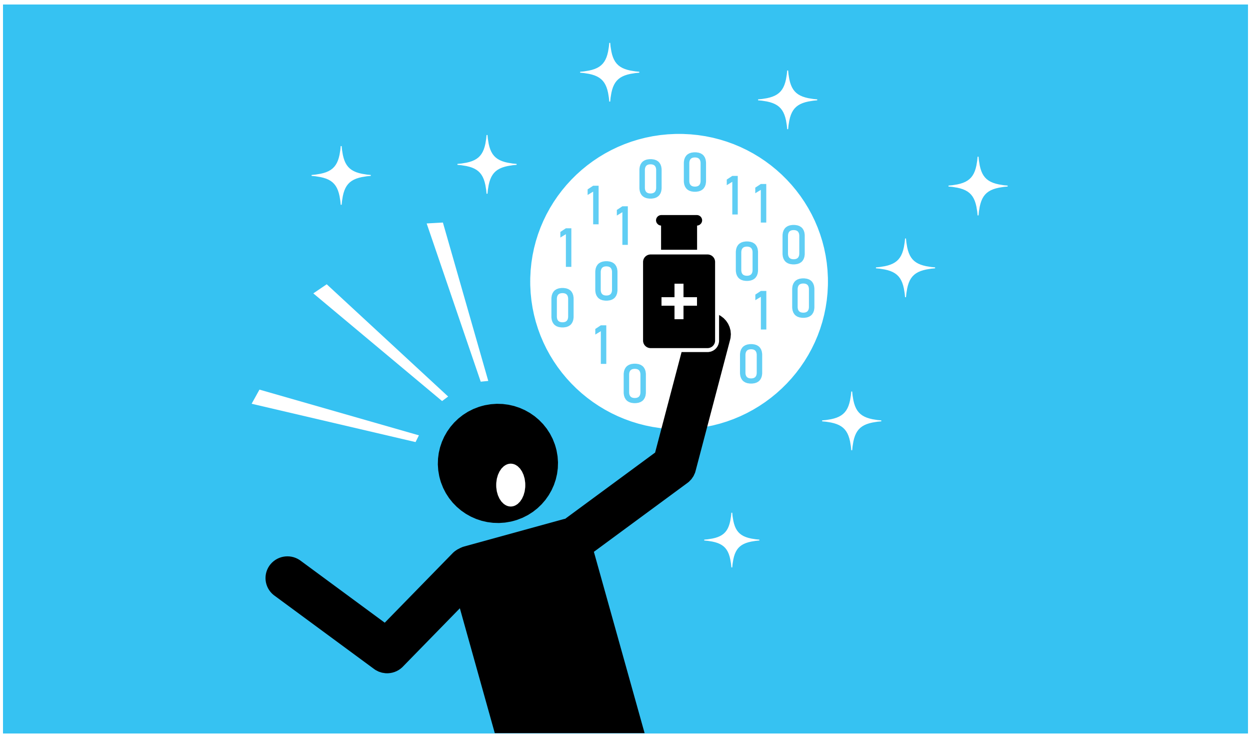
It's extremely risky, as appealing as it may sound, to take the Westphalian concept of sovereignty and translate it with its whole complexity into the digital age.

I am still not sure I understand what people mean when they talk about information sovereignty or Data Sovereignty or digital sovereignty and all these terms being thrown around. There is no system to how they are being used.

If you are a small country, you will never have a full sovereign technology stack.

With the digital and physical spaces coming together, should we continue to use this old, Westphalian model of sovereignty?

DATA SOVEREIGNTY IS PEDDLED AS A **PANACEA TO MANY CONCERNS**



The multifaceted notion of Data Sovereignty is both explained and perceived in very different, sometimes conflicting, ways.

A reaction by states to a sense of loss of control

The reaffirmation of the importance of sovereignty in digital matters is a growing trend in the political discourse of states, beyond the long-time proposnents of the approach. It is in large part a reaction to a perceived powerlessness regarding the enforceability of national laws and accelerating technological and economic competition. Depending on the country, this can be triggered by a diversity of concerns, including: foreign surveillance practices, interferences in internal democratic processes, difficulties to access evidence in criminal investigations or to obtain the removal of illegal content on social media, protection of privacy, the rise of extremely powerful private actors, fears of dependency and vulnerability in a context of increasing geopolitical tensions, or any combination thereof. In this context, sovereignty is a familiar and powerful proxy for reestablishing the paramount authority of states in the digital space and their perception of independence.

A cloud of related concepts

Strongly echoing debates dating back to the 60s and 70s about "information sovereignty"[33] or "cyber sovereignty" driven mainly by Russia and China, expressions appending sovereignty to other notions have proliferated recently. Examples range from the broader terms, often evoked by governments, such as "technological sovereignty", "data sovereignty" or "digital sovereignty", to the more technology-specific, invoked by corporate actors, such as "cloud sovereignty", "operational sovereignty", or even "software sovereignty". Other related terms include "data localization" or "data residency" and also "digital autonomy" and "digital self-determination".[34]

In this competition of buzzwords and expressions, Data sovereignty is clearly gaining traction, albeit more as a political concept than one addressing the concrete legal implications of the exercise of sovereignty in the digital age. Although vague and undefined, it has been used to anchor a variety of technical and non-technical measures for greater ownership and autonomy regarding data.[35]

A multiplicity of policy objectives under the umbrella of Data Sovereignty

Data Sovereignty is invoked by states as a protective or empowerment stance regarding a multitude of stakeholders: their citizens, companies and the state itself. This umbrella notion is understood and presented as a panacea to achieve a whole gamut of interrelated security, economic and human rights as well as social objectives.

Security aspects encompass inter alia: protecting vital infrastructures, securing government and military data critical for national security, preventing surveillance by foreign nations, avoidance of supply chain dependency on technological components, and preventing threats to democracy. Economic goals include: developing local business champions, IT sector employment, repatriation of created value and tax revenues, fostering the development of artificial intelligence, and more generally, a wish to level the playing field with the countries that host the major data-driven companies. Human rights-related objectives include: protecting citizens privacy, fighting against a variety of online abuses (terrorism, hate speech, disinformation) while ensuring the right to access information and freedom of expression.

An appropriation of the concept by other actors

Different understandings of the concept of Data Sovereignty are also emerging either to organize corporate practice or to empower individuals or communities.

Some businesses and particularly cloud providers introduce it as the capacity for their customers to fully control the conditions and purposes under which the provider can access their data, including through the customer's management of its own encryption keys. This is considered without any relation to territories.

In parallel, some actors see the visibility of the concept of Data Sovereignty as an opportunity to promote a vision of "*digital self-determination*" based on the autonomy of individuals and their right to control the data they own or generate. The aspiration of indigenous communities to Data Sovereignty, in response to the United Nations Declaration on the Rights of Indigenous Peoples (UNDRIP) for the collection, ownership and application of data pertaining to indigenous peoples, such as the one promoted by the Global Indigenous Data Alliance (GIDA), is a topical example of an extensive interpretation of the term.

[33] Kuner, C., (2013), *Transborder Data Flows and Data Privacy Law*, Oxford University Press.

[34] Swiss network on Digital Self-Determination (2020), *Promoting Digital-Self Determination*, June 2020, Internet Governance Forum.

[35] Hummel, P., M. Brau, M. Tretter, P. Dabrock (2021), "Data sovereignty: A review", *Big Data & Society*, Vol. 8, Issue 1, https://doi.org/10.1177/2053951720982012.

Data Sovereignty means different things for different people

The proposed definitions of Data Sovereignty are as diverse as the objectives that the term is supposed to achieve, and the numerous actors who try to explain it or use it to justify measures they propose or implement.[36] It is not surprising therefore that the reception of the term is similarly diverse, like a Rorschach test upon which all actors project their own perspective. While to some it represents a positive step toward individual self-determination and the empowerment of users in the digital realm, others see it as a dangerous justification for increased (state) surveillance or protectionism and even bringing a risk of fragmentation of the internet itself. Moreover, within stakeholder groups, and particularly among businesses, actors' reactions vastly vary according to how much direct benefit or constraints they expect from the proposed measures.

Quotes from consulted stakeholders

When we say yes to all of the dimensions of these emerging concepts, anyone can read whatever they want into them, which is not helpful at the policy level.

The meaning of Data Sovereignty varies quite a lot across stakeholder groups and even within stakeholder groups, ranging from the idea of personal self-determination to states exercising control.

Using Data Sovereignty as a blunt tool to prevent the international flow of data is effectively an anti-globalization measure.

It's unfortunate that the same term is used for sovereignty of nations, sovereignty of a region, from infrastructure to control of data and, as well as for privacy or sovereignty of the individual to control their own data. And we have to resolve that.

We need to get past "Data Sovereignty is the answer"; what's the question?

Data Sovereignty makes a great bumper sticker but does not necessarily make for great policy.

We need to get some sort of sense of whether or not, Data Sovereignty is actually anchored in international law, or if it's something entirely different, perhaps something just political.

These measures are the example of weaponization of regulation to increase market share of national champions.

Everyone chooses to talk about Data Sovereignty and regulation because those are the things we think we are allowed to use. As opposed to talking about the actual underlying issues which is that we don't have trust. And then we retreat to nationalism and the self-reassuring thought that 'at least the data is in my country'.

Data Sovereignty should not be misunderstood as data isolation.

Data Sovereignty has become a sort of Rorschach test, where everyone can read into the concept whatever pleases them and serves their purpose in a given context.

[36] Idem.

IMPLEMENTATION **PITFALLS**

Data Sovereignty measures come in different guises, and their implementation is prone to unintended consequences, with systemic effects if generalized.

A diversified arsenal of Data Sovereignty measures

Generally for states, the key objective of Data Sovereignty measures is to ensure applicability and full enforceability of national laws by leveraging or establishing some nexus of connection with the territory. Data Sovereignty may take the shape of data localization provisions in laws and regulations, but also of less evident measures in the form of licensing provisions and contractual requirements. Rules can thus be based on: the location of storage and processing (however difficult it may be to pinpoint); the location of users (e.g. EU GDPR, and criteria regarding "provision of services"); or on the location of the operator (e.g. the extraterritorial provisions of the U.S. Cloud Act, or obligations of local representation). More rarely because of compliance complexity, but more interestingly though, instead of focusing on a connection to the territory, measures can establish limits regarding the use or re-use of collected data. This can be in particular in privacy or sectoral regulations.

In parallel, concrete state measures under the label of Data Sovereignty come in many guises, impacting data flows directly or indirectly. Some distinctions can help categorize them, while recognizing they may not be mutually exclusive.

First, in terms of direction of data flows, like trade is differentiated between import and export, Data Sovereignty measures either address data *coming* in the territory (e.g. compulsory gateways, blocking, VPN bans), or *going out* of the country, via limits on certain categories (e.g. defense, government, or health data) or a general mandatory localization. A second distinction, related to the nature of data, is naturally between personal and non-personal data, with a major focus on the former, despite the blurring boundaries between the two. Finally, these measures can have extraterritorial or only national effects, depending on the norm-setting power and intent of the initiator.

The devil of implementation is always in the details

Data Sovereignty measures, like any thematic legal framework, must achieve a balancing (or ideally reconciling) of competing interests through a complex set of precise and interlinked provisions. Each of these provisions can have major consequences during actual implementation. The devil always lies in the details: small parameter changes can turn a justified regulatory approach into an ineffective or even dangerous tool.

As an illustration, privacy regulations set parameters regarding limits to collection and reuse. They will not ensure the desired result if too lax but may introduce excessive burdens and make ensuring compliance difficult if too strict or rigid. Likewise, depending upon their workflow and procedural guarantees, regimes for cross-border access to electronic evidence may either vastly improve the security of citizens or subject them to intrusive surveillance. Similarly, states' redefinition of the role of platforms in content moderation can establish a mutually beneficial framework or incentivize social media companies to ramp up private censorship.

In this regard, irrespective of their potential risks, data localization provisions have different impacts if they apply to all data or only some categories, and whether they impose a full prohibition of foreign transfer, an obligation to exclusively store in-country with foreign access allowed, or only the storage of a copy. Ultimately, different measures related to Data Sovereignty are constantly changing and being immersed in complex sector-specific regulations, which renders implementation and compliance increasingly difficult, particularly when technological developments are considered.

Unintended consequences are to be anticipated

The inaccessibility of some news sites from the United States for European citizens, and the intense political polarization in the United States are unintended (and surely unanticipated) consequences of, respectively, the European Union GDPR and algorithmic recommendations on social media.

Likewise, Data Sovereignty measures, as many policy decisions about complex ecosystems, are prone to unintended consequences. Because of international dynamics and the reactions of other actors, such unilateral initiatives are highly likely, in a boomerang effect, to produce results different or even contrary to the initiator's intent and detrimental to local actors, particularly small ones.

Security-wise, sub-par levels of protection on smaller local clouds can make them more vulnerable to attacks and potentially devastating leaks than large-scale infrastructures. Threats are often domestic. Data localization can substantially undermine digital security when mandating that data is stored in one physical location. It also risks weakening fraud prevention and anti-money laundering solutions.[37]

In addition, useful foreign-based services can be incentivized to avoid markets with excessive local constraints, to the detriment of local citizens and businesses. Mandating data to stay within a national border and requiring its unnecessary duplication has an economic and ecological cost. For some data flows, even milliseconds matter.[38] Moreover, research shows that data localization and associated regulations on the free flow of data tend to reduce productivity and economic output in those industries that depend relatively intensively on data services. Local businesses can in addition be hampered in their own international development, due to ripple effects along local value chains. Efforts to strengthen a particular local sector (e.g. data centers) may also collaterally harm other sectors, including AI and Machine Learning requiring massive training data sets.

[37] Institute of International Finance (2020), *Data Localization: Costs, Tradeoffs and Impacts Across the Economy*, www.iif.com/Portals/0/Files/content/Innovation/12_22_2020_data_localization.pdf.

[38] Deloitte Digital and Deloitte Ireland (2020), *Milliseconds Make Millions*, www2.deloitte.com/ie/en/pages/consulting/articles/milliseconds-make-millions.html.

Systemic impacts are likely if measures are generalized

States are tempted to reaffirm their sovereignty through unilateral extraterritoriality, incentivizing others to do the same. Ironically, not only does it weaken the very principle of non-interference but it also exposes the initiator to being later on the receiving end of similar or retaliatory measures by other, often more powerful, states. Such a legal arms race,[39] marked by increasing conflicts of laws, makes interoperability and cooperation even harder. Moreover, the Data Sovereignty rhetoric adopted by democratic countries, if done without caution, allows repressive regimes to misappropriate the concept and mandate data localization for surveillance purposes under the alibi of data protection. Instead of fostering competition, a global race towards data localization could ultimately strengthen the position of large global companies: only they would be able to afford duplication of infrastructures in every market and the costs of compliance, unlike smaller innovative ones that could become confined to their own local markets. It also creates barriers to international data sharing, which is particularly pressing in a context of emerging global challenges, such as pandemics and climate change.

Last but not least, tampering with the architecture and routing of the internet can reduce its global resiliency, impact its security and lead to sub-optimal network investments.

[39] De La Chapelle, B. and P. Fehlinger (2016), "Jurisdiction on the Internet: From legal arms race to transnational cooperation", *Paper Series*, No. 28, Global Commission on Internet Governance, www.cigionline.org/sites/default/files/gcig_no28_web.pdf.

Quotes from consulted stakeholders

There are big speeches around Data Sovereignty, but the actual implementation is very different.

Implementing the concept of sovereignty on the digital economy requires having control and borders applicable to digital assets.

There is this idea that if we insist on data localization, cloud companies will come and build data centers in our country. They don't. Data localization is hardly enforceable.

So it goes beyond how and where data is stored, but applies to what data is allowed (speech controls), in what form it may be transmitted and stored (data restrictions and data localization), who may access it (surveillance), and finally how it may be used (data protection/misuse).

We should not imagine that we can embed a single set of rules and they will apply uniformly throughout the internet because of all their variations that takes place there, including in the geographic and ethical dimensions.

Data Sovereignty is really detrimental to the future of the internet, and even more importantly the cloud, and even more importantly the cloud of things.

What engineers designing the internet standards focus on is performance, reducing latency and securing the network. The more constraints you put around, such as where the data can be located, the harder it gets to achieve your objectives, when you're suddenly constrained by a geography that the network itself is oblivious to.

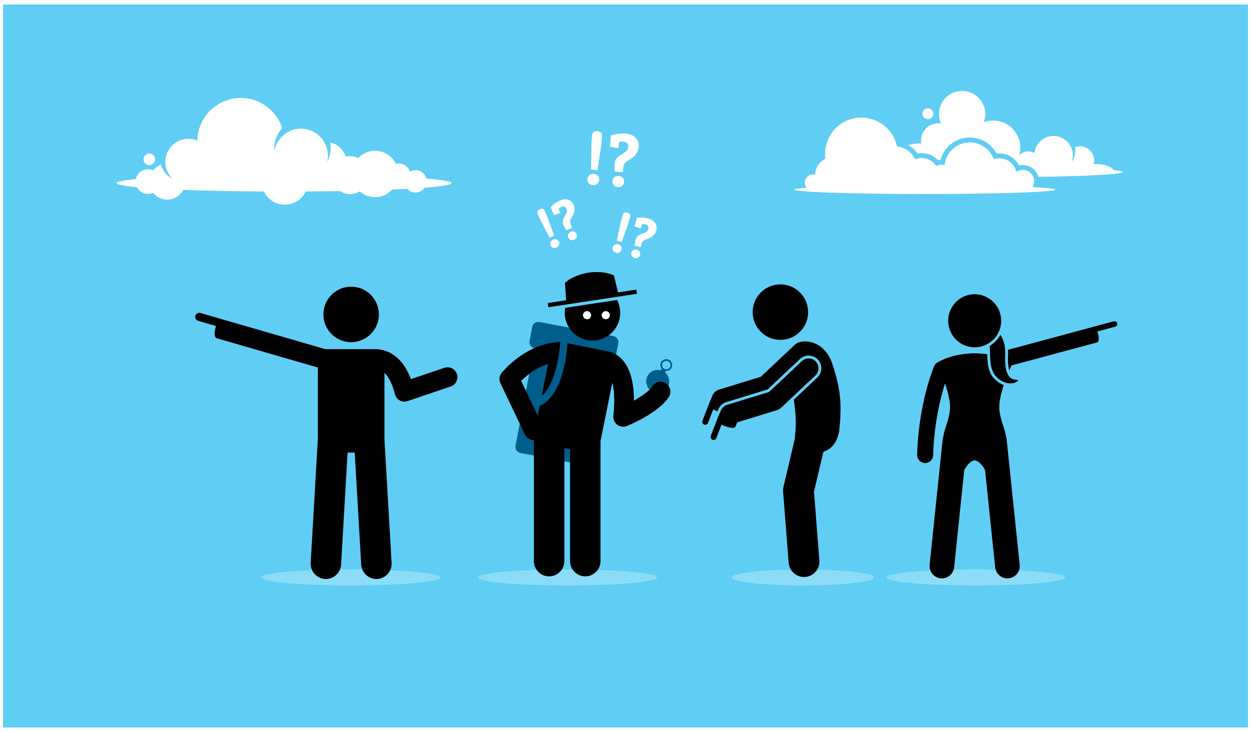
There are just too many things conspiring to lead to a splinter cloud.

I believe that the majority of the countries may not be aware of the implications of sovereignty measures.

If everyone implements that then there will be a race to the bottom.

If every country had Data Sovereignty rules, perhaps they would need to work harder to find some way to make global business still functional.

DEALING WITH MULTIPLE JURISDICTIONS



Data connects with territories and jurisdictions in multiple ways, producing an ecosystem of overlapping applicable rules and redefining the exercise of sovereignties.

A plurality of territorial nexus

There are numerous ways in which data connects to territories. It may be through the location of individuals or entities the data originates from (either through collection or voluntary production), but also through the county of incorporation of the entity(ies) that control or process this data, as well as the location of who is entitled to access it or the resulting service. Accordingly, several state entities can have some ground for prescriptive, adjudicative or even enforcement jurisdiction.

In addition, the growing exercise of extraterritoriality by states in digital matters, through unilateral regulatory action or the affirmation of personal jurisdiction by courts, make a state's citizens and businesses increasingly subject to foreign rules. One can also argue that the increasing importance of the terms of service of global platforms introduces a normative plurality that makes the reconciliation of competing norms and standards more complex.

Overlapping applicable rules

The multiplicity of potentially applicable rules introduces high legal uncertainty for all actors, states as well as businesses and citizens. Moreover, globally active businesses may be caught in conflicts where abiding by the laws of one country makes them in breach of that of another.

In parallel, foreign private entities have been entrusted with the responsibility to de facto adjudicate and implement national legislations, as in the recent NetzDG[40] in Germany regarding content moderation on social media platforms, or the right to be de-indexed on search engines in application of the Costeja case of the CJEU[41].

More generally, dealing with digital activities often entails combining different sets of rules, rather than the classic choice of law situation, where the question is rather which (single) law is applicable to a particular situation.

Controversies regarding choice of forum clauses in early terms of service illustrate the reticence towards excessively simplifying solutions. The relatively rarely used concept of comity might find there a novel, and maybe extended, application.[42]

Rights but also responsibilities of states

The usual definition of sovereignty as supreme authority over a territory remains fully applicable whenever the effects of legislations are limited to the geographic borders of the state. Yet, this is an increasingly rare condition when dealing with data. It therefore behooves states, to exercise restraint and responsibility regarding the potential trans-border impacts of their exercise of sovereignty, in line with the principle of non-interference. Such a principle of responsibility is actually not new. Indeed, Article 35 of the Tunis Agenda of the World Summit on the Information Society (WSIS) in 2005 states: "*Policy authority for internet-related public policy issues is the sovereign right of States. They have rights and responsibilities for international internet-related public policy issues*".[43] The presence of two sentences clearly corresponds to the distinction above between full authority over one country's territory and rights but also responsibilities for transnational issues.

This approach could point in the direction of the legal solutions already implementing varying degrees of sovereignty for waters, airspace, the lithosphere, and outer space. It has been suggested that the Datasphere, considered as a space, might just be "in need of law", i.e. of a meta-framework organizing the coexistence of several jurisdictions over this shared space.[44]

[40] BMJV (2017), "Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act)", Bundesministerium der Justiz und für Verbraucherschutz, https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf.

[41] CJEU (2014), "Case C-131/12 Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja Gonzaléz", Judgement of Court (Grande Chambre) of 13 May 2014, https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A62012CJ0131.

[42] Garner, B. A. (2014), "Comity", *Black's Law Dictionary*, 10th Edition, Thomson Reuters.

[43] UN and ITU (2005), *Tunis Agenda for the Information Society*, World Summit on the Information Society, https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html.

[44] Bergé, J.S., and S. Grumbach and V. Zeno-Zencovich (2018), "The 'Datasphere', Data Flows Beyond Control, and the Challenges for Law and Governance", *European Journal of Comparative Law and Governance*, Vol. 5, Issue 2, https://ssrn.com/abstract=3185943.

Redefining sovereignty(ies)

As seen earlier in this report, evocation of Data Sovereignty also triggers mentions of rights beyond those of states: for operators and business users of cloud services, but also for communities (e.g. indigenous ones), and individuals. Initiatives are emerging accordingly to propose innovative data stewardship models (e.g. data commons, cooperatives, trusts, collaboratives, fiduciaries, and marketplaces).[45]

In its strategy on digital policy, Switzerland has introduced the concept of digital self-determination.[46] The insertion of this concept in the debate about sovereignty in the digital age may, therefore, open up additional avenues for exploration. It starts bottom-up with the rights of the individual and then up the chain of his/her participation in various nested groups.

Could a notion of responsible self-determination serve in that spirit as a basis and focal point[47] allowing the self-organization of human communities in the digital age? This would be more reflecting of the complex hypergraph[48] structure of humanity than its simple partition in a limited number of geographically-determined nation states.

In a concrete way, a distribution of responsibilities between states, online platforms and users has been proposed[49] in a layered and nested way through the distinction of regulation *of* platforms (by states), regulation *by* platforms (of their users through terms of service), and *on* platforms (by the administrators of forums and groups).

The development of a set of guidelines on acceptable parameters and guardrails that could serve as a baseline for interoperability discussions would be useful. Ultimately, what matters is who has the power and ability to set, adjudicate and enforce rules and this is more widely distributed among actors than ever in the digital era. Significant innovation in governance is needed to deal with this major challenge.

[45] Mozilla Insights (2020), *Shifting Power Through Data Governance*, https://foundation.mozilla.org/en/initiatives/data-futures/data-for-empowerment/#10-data-governance-approaches-explored.

[46] Strategy Digital Policy Switzerland (2020); www.digitaldialog.swiss/en/; see also: Swiss network on Digital Self-Determination (2020), "'Promoting Digital-Self Determination'", June 2020, Internet Governance Forum, https://www.intgovforum.org/multilingual/index.php?q=filedepot_download/10271/2243.

[47] A term coined by Nobel Prize-winner Thomas Schelling in game theory for cooperative games. See: Schelling, T. C. (1960), The strategy of conflict, Harvard University Press, Cambridge.

[48] Wikipedia (n.d.), "Hypergraph", https://en.wikipedia.org/wiki/Hypergraph.

[49] Internet & Jurisdiction Policy Network (2019), "Content & Jurisdiction Program Operational Approaches", https://www.internetjurisdiction.net/outcome/content-jurisdiction-program-operational-approaches.

Quotes from consulted stakeholders

When we use the phrase Data Sovereignty, it's not clear if you're talking about hard Data Sovereignty: data from our citizens will stay in the country, period, exclamation point. Or if it means soft Data Sovereignty: a copy of our citizens data will be available to our government if we need it, but it can go anywhere it needs to go.

It might be helpful to try to describe what properties we want to preserve or protect (freedom of expression, access to information) while recognizing that we may also want to provide for protection of populations from harm.

It is not easy to reach a common understanding on these topics. Even when we look into common principles, they have different implementations in different jurisdictions.

There are a lot of other conflicts that show up just because rules are adopted by different jurisdictions. And companies are struggling to figure out how to build a system that meets these potentially conflicting requirements.

We have standard-setting processes that are not open to all and are creating de-facto standards. The GDPR, for example has become a de facto standard. This is concerning for other regions in the world that have not participated in this process.

We need to understand who has interests in the data, and when those interests are in conflict.

There needs to be clarity in terms of what is a legitimate restriction.

We need to build an upgrade versioning paths to our policies and regulations. Lawmakers should steal methodology from software development. We pass budgets every year, why don't we pass data regulations every year? So we can be flexible and responsive on the concrete cases. And only every five years revisit definitions, which are more useful when stable.

*We need a framework that addresses internet governance holistically. One of the mistakes we have made in the last 30-35 years of internet regulation is trying to deal with each issue (content moderation, privacy, cyber security, national security/public safety) in silos. When we do that, we fail to account for how a mitigation for one concern *creates* new problems in other areas, and oftentimes the solution creates new tensions between fundamental human rights.*

There is no forum of discussion for these issues. We need standards and frameworks for the topic of cross-border data flows.

CHAPTER

4

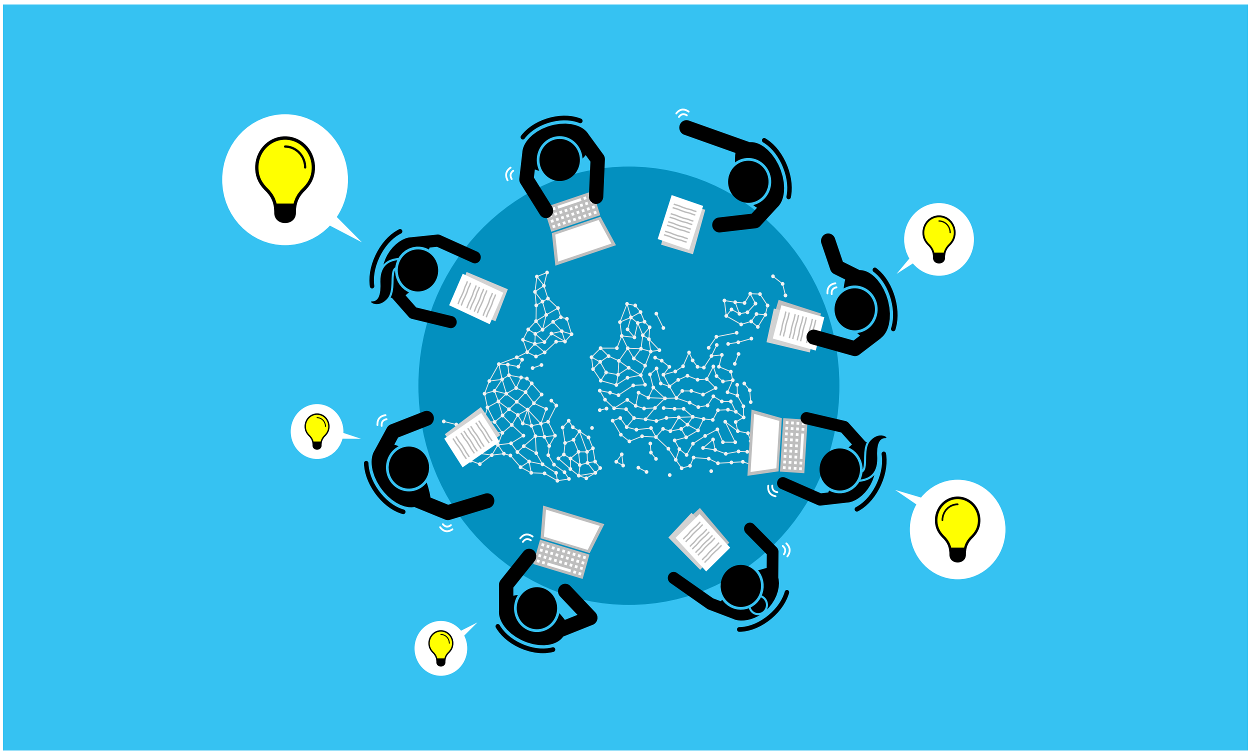
MOVING FORWARD

In managing, promoting and protecting [the Internet's] presence in our lives, we need to be no less creative than those who invented it. Clearly, there is a need for governance, but that does not necessarily mean that it has to be done in the traditional way, for something that is so very different.

KOFI ANNAN

- *Organizing a global multistakeholder debate across sectors*
- *Reframing the discussion towards more nuance and common objectives*
- *Exploring and fostering innovative approaches*

MOVING FORWARD



A global multistakeholder debate across sectors needs to be organized, to reframe the discussion and to explore innovative approaches in tools, frameworks and concepts for dealing with data.

The debate between Free Flow of Data and Data Sovereignty has never been more polarized. On one side are defenders of unrestricted flow of data, given its positive effects on innovation and the digital transformation of economies and societies. On the other, proponents of states and data subjects want to reclaim full control over data, given the plethora of concerns surrounding data use. More than ever, nuance is needed.

Balancing between different uses, sectors and stakeholders is indeed challenging, in particular to ensure fairness among stakeholder groups and within stakeholder groups. However, a minimum starting point is to establish a common understanding of the vocabulary employed. It is also about bringing to light what the actual, and legitimate, competing objectives are - be they related to human rights, economy and security - in a context where data becomes increasingly relevant for all. Properly framing the debate means addressing both substance and methodology.

There are recent efforts to find formulations that reflect this desire for reconciliation and nuance. Some can be seen at the multilateral level, e.g. in the G7 and G20 ("Data Free Flow with Trust" [DFFT] led by Japan in the Osaka Track, which aimed to inaugurate a new negotiation track for data governance) and at its organizations (e.g. the OECD through its work on "Trusted flows of personal data").

To move forward, the different actors need to engage in a creative discussion that is more global, evidence-based and focused on common objectives.

Organizing a global, multistakeholder debate across sectors

Due to the unique nature of data and data flows, as well as to the multiplicity of jurisdictions involved, unilateral measures to address legitimate concerns around Free Flow of Data cannot suffice. More coordinated action is needed in order to promote interoperability and ensure that well-being is maximized for individuals and societies. This is about enabling societies to take advantage of what technology can offer, while limiting the potential negative dynamics it may entail.

In order to move forward, we need a debate that is global. Given the interdependencies and the global architecture of the internet, the discussion around the future of cross-border data flows cannot be limited to only a few countries of the world. However difficult this is, it is necessary to include all regions in this crucial debate, and most importantly, to ensure that developing countries and smaller actors are able to actively engage in the discussions. Information on the complexity of the issues and what is at stake must be available to all. Knowledge and understanding of characteristics of data, its collection, processing and use, need to be socialized to foster transparency in the conversations society has on this matter, as well on the decisions it makes.

Such a process also needs to ensure that not only states, but also other stakeholders, such as the private sector, civil society and technical community can equally participate in designing, developing and ultimately implementing any proposed approach. It is crucial that the debate is also intergenerational. All existing multistakeholder fora should be leveraged in this context.

But most importantly, the data discussion is one that goes beyond technical discussions related to the internet and one that is too often conducted in silos. Without dismissing their contributions to advancing specific elements of the debate, a more systemic approach that builds on the lessons learnt from existing discussions and on collective intelligence is needed. Data touches all policy areas, economic sectors and increasingly more dimensions of life. Establishing a global cross-sectoral multistakeholder debate is crucial to moving forward.

Reframing the discussion towards more nuance and common objectives

This report is a preliminary effort to provide all actors with a shared basis for further exchanges on solutions to what is ultimately their common challenge: addressing the future of cross-border data flows to the benefit of all. During the consultations, some key elements have emerged, summarized here to help structure future discussions.

First, this increasingly important debate addresses a uniquely complex and novel issue, due to:

- ***The unusual characteristics of data:*** the massive volumes at stake, its non-rivalrous nature, the inherently transnational aspects, and the complexity of its value chains.
- ***The diversity of uses across all sectors:*** this matters more than the purely technical transport or storage and processing locations.
- ***The numerous norm-setters involved:*** not only states but also businesses and citizens interact in unprecedented ways across borders.

Some cautionary messages also emerge when seeking to unpack the concepts of Free Flow of Data and Data Sovereignty:

- ***Analogies should be used wisely:*** Analogies are useful to approach unfamiliar situations related to data, but taking them too literally can lead to misguided policy choices.
- ***Legitimate concerns must be addressed:*** They overlap security, economic and human rights dimensions, as consequences of growing digital interdependence.
- ***Implementation pitfalls should be considered:*** The devil is in the details, unilateral measures

concerning data can have unintended consequences and their generalization may be damaging.

Some common objectives could guide efforts to address these complex challenges:

- ***Maximizing the wellbeing*** of individuals and societies, with a fair distribution of economic and social benefits, and obligations.
- ***Addressing concrete issues*** and bridging currently separated silos that prevent the understanding of interrelations between sectoral approaches.
- ***Defining the distribution of responsibilities*** among actors regarding who can prescribe, adjudicate, and enforce rules to organize the Datasphere.

Exploring and fostering innovative approaches in tools, frameworks and concepts

We are confronted with a civilizational challenge: organizing the coexistence and interactions of billions of people and entities, with vastly different interests, connected through the internet and a global Datasphere. Key questions therefore emerge: What is the digital society we collectively want to build? Under which principles and norms? What are the mechanisms, normative or technical, that will allow us to collaboratively address the issues that we are confronted with? In that regard, building the methodology for addressing new problems is almost as important as developing concrete solutions to them.

The scope and depth of the current challenges demonstrate the limits of the existing frameworks. Significant innovation is therefore much needed, regarding both the tools and the institutional mechanisms we rely on.

As evoked in the report, innovation is already under way and should continue to be fostered in at least three dimensions:

- **Technical solutions.** This is an emerging dynamic sector. Not all solutions will come from regulation, many will likely come from new technological innovations emerging to foster trust. These include: hybrid use models (e.g. public data for private use, private data for public use); new stewardship approaches (e.g. data commons, cooperatives, data trusts, data collaboratives, data fiduciaries, data marketplaces, indigenous data governance etc); digital identity schemes; or blockchain-based applications.

- **Normative frameworks.** This is not primarily about imposing traditional rules on a new and rapidly evolving reality. It is also, more importantly, to continue the ongoing adaptation of the international legal architecture, as was done repeatedly with the advent of new disrupting technologies. Specific transnational regimes are under discussion to address specific issues such as cross-border access to electronic evidence, content moderation on large global social media platforms, or privacy protection. More will be needed. The challenge, however is to ensure the interoperability between frameworks adopted separately and often unilaterally.

- **Concepts.** The proliferation of terms to define objectives illustrates a situation of paradigmatic crisis in the sense of Thomas Kuhn[50] and the aspiration to search for new concepts that explain a situation with more clarity and guide the development of future efforts. The present report has mentioned some, such as: *Free Flow of Data with Trust, Digital self-Determination* or the

[50] Kuhn, Thomas S. (1970), *The Structure of Scientific Revolutions*, University of Chicago.

notion of a *Datasphere*. They may not be definitive, but point in the direction of more conceptual creativity.

Finally, significant governance innovation[51] is also required, in order to:

- **Enable experimentation** through, for example, regulatory sandboxes[52], nested regulations hybrid approaches, regulated self-regulation,[53] and novel dispute-resolution arrangements.

- **Ensure that frameworks are future-proof**, given that the data economy is a new sector in full development, many new services and technologies will likely emerge around data, just like the invention of the web produced a plethora of new activities and businesses.[54]

- **Enable interactions** and bridge silos among sectoral institutionalized processes that address interdependent issues from different perspectives and interests.

Organizing ongoing global interactions in a way that reduces mistrust among stakeholders and allows them to partake in the building of concrete solutions is difficult. There is a procedural vacuum that needs to be addressed.

This requires a new type of transnational cooperation, which may ultimately entail the creation of new institutions.

> *A core goal of public policy should be to facilitate the development of institutions that bring out the best in humans.*
>
> **ELINOR OSTROM**

[51] Ministry of Economy, Trade and Industry (2019), Japan (METI). *Governance Innovation: Redesigning Law and Innovation in the Age of Society* 5.0., Japan, 2019. www.meti.go.jp/english/press/2019/pdf/191226001.pdf; Ministry of Economy, Trade and Industry (2020), Draft Report *Governance Innovation ver.2: A Guide to Designing and Implementing Agile Governance*, Japan, https://www.meti.go.jp/english/press/2021/pdf/0219_004a.pdf.

[52] Attrey, A., M. Lesher and C. Lomax (2020), . "The role of sandboxes in promoting flexibility and innovation in the digital age", *Going Digital Policy* Note, No. 2. 2020, https://goingdigital.oecd.org/toolkitnotes/the-role-of-sandboxes-in-promoting-flexibility-and-innovation-in-the-digital-age.pdf`.

[53] Hoffmann-Riem, W. (2001), *Modernisierung in Recht und Kultur*, Suhrkamp, Frankfurt.

[54] WEF (2020), *A Roadmap for Cross-Border Data Flows: Future-Proofing Readiness and Cooperation in the New Data Economy*, www3.weforum.org/docs/WEF_A_Roadmap_for_Cross_Border_Data_Flows_2020.pdf.

INTERNET & JURISDICTION POLICY NETWORK

The Internet & Jurisdiction Policy Network is the multistakeholder organization fostering legal interoperability in cyberspace. Its stakeholders work together to preserve the cross-border nature of the internet, protect human rights, fight abuses, and enable the global digital economy. Since 2012, the Internet & Jurisdiction Policy Network has engaged more than 400 key entities from six stakeholder groups around the world including: governments, the world's largest internet companies, the technical community, civil society groups, leading universities and international organizations.

The regular Global Conferences of the Internet & Jurisdiction Policy Network are institutionally supported by six international organizations: Council of Europe, European Commission, ICANN, OECD, United Nations ECLAC, and UNESCO. Host partner countries include France (2016), Canada (2018) and Germany (2019).

The Community

6
STAKEHOLDER GROUPS

70+
COUNTRIES

400+
ENTITIES

STATES

INTERNET COMPANIES

TECHNICAL OPERATORS

CIVIL SOCIETY

INTERNATIONAL ORGANIZATIONS

ACADEMIA

Mission

INFORM

The debates to enable evidence-based policy innovation

Informational asymmetry and mistrust between actors often result in uncoordinated policy action. The I&JPN facilitates **pragmatic** and well-informed policy-making by framing issues and taking into account the **diversity of perspectives** while documenting tensions and efforts to address problems.

CONNECT

Stakeholders to build trust and coordination

Cooperation is important in a digital environment that is increasingly polarized, and where actors function in policy silos, with insufficient factual information.
The I&JPN serves as the **connective tissue** between stakeholder groups, regions, and policy sectors, as well as by **bridging gaps** within governments or organizations.

ADVANCE

Solutions to move towards legal interoperability

The Policy Network strives to develop shared **cooperation frameworks** and **policy standards** that are as transnational as the internet itself. The Network promotes a **balanced and scalable approach** to policymaking, aiming for legal interoperability, taking inspiration from the fundamental principle that enabled the success of the internet and the World Wide Web.

Core activities

POLICY PROGRAMS

EVENTS

KNOWLEDGE MUTUALIZATION

www.internetjurisdiction.net